IAM Cheat Sheet

by iddd via cheatography.com/197744/cs/41898/

What is...

What is Identity and Access Management ? IAM is about making sure that the right person has access to the right resources and information within the organization, through the combination of systems, policies, processes and technologies.
Granting or denying access requires 3 things: object, request and identification.

Related acronyms

ACL	Access Control List	Defines who can access an object/document/info and what operations they can perform
AD	Active Directory	Directory servicce by Microsoft
API	Application programing interface	Set of rules and protocols that allow different software applications to communicate and interact with each other. They specify how softwrae components should interact, enabling the exchange of data and functionality between systems.
AS	Authentication server	Server responsible for authenticating users in a network, often part of a centralized authentication system
BaaS	Backoffice as a service	BaaS providescloud-based backend services, such as databases and storage.
BYOD	Bring your own device	Policy that allows employees to use their personal devices for work-related tasks
BYOID	Bring your own identity	Allows users to use their existing digital entities from external soruces to access applicatios and services
BYOC	Bring your own credential	Allows users to bring their own authentication credentials, often associated with federated identity management
CICD	Continuous integrationg, continuous deployment	Practice that involves automatically testing and deploying code changes to improve development efficiency.
CAPTCHA	Completely automated public turing test to tell computers and humans apart	Security measure to distinguish between human and automated access by requering users to solbe a challenge
CIAM	Customer identity and access management	Subset of IAM that focuses on managing customers' identities
CIP	Customer information programme	Processes and procedures for verifying identity of customers, ofen mandated by regulatory requirements
CORS	Cross-origin resource sharing	Security feature implemented by web browsers to control how web pages in one domain can request and interact with resources hosted on another domains
CSP	Cloud service provider	Company that delivers cloud computing services (including IAM solutions)

Related acronyms (cont)

CSPM	Cloud security posture management	Continuous monitoring and management of an organization's cloud security posture (including IAM configurations)
CTF	Centralized token federation	Centralization of authentication tokens to enable seamless authentication across multiple applications. A token is a piece of data that represets authorization granted for a specific action (it's like a digital key that allows access to certain resources/actions; a proof of authorization)
DLP	Data loss prevention	Set of technologies and strategies designed to preventunauthorized access, sharing, and distribution of sensitive data
EAC	Enrerprise access control	Controlling access to an organization's resources and data, ofthen through a combination of policies and technologies
EAL	Evaluation assurance level	Numerical ratign assigned to IT products/systems to indicate the level of trustworthiness as evaluated by common criteria
EIAM	Enterprise identity and access management	IAM solutions designed to meet the needs of large complex enterprses
FIDO	Fast identity online	Open standard for oline authentication that promotes the use of passwordless and strong authentication methods
FIM	Federation identity management	Approach that enables the portability of digital identities across multiple identity management systems or domains. Relies on methods like biometric authentication, securiy keys and mobile-based authentication
IaaS	Infrastructure as a service	Provides virtualized computing infrastructure
IAG	Identity and access governance	Processes and tehcnologies used to manage and audit user access across an oranization's IT systems
IAMaas	Identity and access management as a service	Tipically cloud-based service that provides IAM management functionalities
IAMCP	Identity and access management compliance program	Complaince program that ensures IAM solution adhere to industry standards and regulations
IAMN	Identity and access management network	Network architecture specifically designed for IAM purposes
IAMU	Identity and access management unit	IAM dedicated unit or team within an organization

Related acronyms (cont)

IDaaS	Identity as a service	Cloud-based services thta provide IAM management functionalities
IdP	Identity provider	System responsible for athenticating and providing identity information for users, tipically used n the contex of federated identity management, in which they may issue security tokens containing user attributes
IDV	Identity verification	Process of verfying the identity of a individual, typically thorugh the use of various authentication methods and checks
JML	Joiners, movers and leavers	Key HR process of handling employees.
KBA	Knowledge based authentication	Asking the individual to provide specific pieces of information that only legitimate owners of the identity would know (eg: personal detials, answers to security questions)
KYB	Know your business	Processes and checks used by organizations to verify and understand the business they are delaing with, often related to anti-fraud and compliance efforts
KYC	Know your customer	Regulatory process that involves verifying the identity of customers to prevent fraud, money laudeting and other illicit activiies
MDM	Mobile device management	Monitoring, managing and securing mobile devices within an organization
MFA	Multi factor authentication	Extra layer of security that requires users to provide multiple forms of identification before granting access
OTP	One time password	Password that is valid for one login session transaction, commonly used in 2 fatcor authentication
Paas	Platform as a service	Provides a platform allowing cusotmers to develop, run and manage applications
PAM	Privileged access management	Managemen of accounts that have unusual or elevated access
PII	Personally identifiable information	Info thta can be used to identify a specific individual (name, address, social security n.,..)
PKI	Public key infrastructure	Framework that manages digital keys and certificates, enabling secure communication and authentication in a network

Related acronyms (cont)

RFID	Radio-frequency identification	Uses radio waves to identify and track objects equipped with RFID tags, often used for asset tracking and access control.
Saas	Software as a service	Software applications delivered over the internet on a subscription basis, allowing users to access the software wihtout the need for local isntallation and maintenance
SCIM	System for cross-domain identity management	Standard for automating the exchange of user identity info between systems, simplifying user provisioning and management
SIEM	Security information and event management	Approach to security management that combines security information management (SIM) and security event management (SEM) to provide real-time analysis of security alerts
SOD	Segregation of duties	Security concept thta involves distributing task and privileges among multiple individuals to prevent conflicts of interest and reduce the risk of fraud
SP	Service provider	Entity that host services or resources. Rely on IdPs to grant access
SS	Service server	Serer thta provides a specific service, often in the context of IAM, where it may handle authentication, authorization, or other identity-related functions
SSA	Security standards and agreements	Defininf and implementing security standards and agreements related to IAM within an organization
SSO	Single sign on	Authentication process that allows a user to access multiple applications with a single set of login credentials
TGS	Ticket granting server	Server that issues TGTs for user authentication. Component of Kerberos authentication.
TGT	Ticket granting ticket	Ticket obtained from the AS used to request a service ticker from the TGS. Part of the Kerberos authentication system.
UBA	User behavior analytics	Analyzing patterns of user behaviour to detect and respond to anomalies that may indicate security threats
UEBA	User and entity behavior analytics	Advanced form of UBA that includes the analysis of both user and entity behaviour to identify potencial security incidents

Related acronyms (cont)

U2F	Universal 2nd factor	Open authentication standard that strengths and simplifies two-factor authentication using specialized security keys

Concepts

Identification

> •Establishing an identity (applicant > claim identity> assured identity). •It may not need to identify **who** you are, but if you're **human**. •Offers assurance, we're looking to control access and establish accountability (there's a need to define what level of assurance do we need (there are 4). e.g.: shared keys or tokens offer a low level of uniqueness.**•An account isn't the same as an identiy! An identity may have multiple accounts!**

Identification proofing

> •Is the process of validating an identity to ensure they are who they claim to be.•Helps to tailor the level of assurance (**How do we know you are who you say you are?**). •Also known as identity verification •Common methods include document verification (passports, driver's licenses, id cards...), biometric authentication (fingerprints, facial or voice recognition...), knowldge based authentication (answers to security questions or personal details...), social authentication (verifying an individual's identity through their social media or other online presence), mobile authentication (one-time codes, mobile apps...).

4 levels of identity assurance

> **1**- there's no need for the identity to be proven; user gives at least one unique identifier. **2-** Claim identity with evidence that supports real world existence (real person); the evidence is protected using cryptographic methods sporting integrity and authenticity. **3-** same as n2 + physically identifying the person to ensure that it's a real person AND the owner of the identity; e.g.: financial identity checks: the name of the claimed identity must match the personal name. **4-** al requirements of the others + subjected to other evidences such as biometrics or photograph to establish the identity

Authentication

> •Process of confirming the identity of an individual when access to a restricted security zone is attemped. **•Authentication factors** depend on the requirements: single (username, pin), dual (username+password), MFA (username+password+mobile device). **•Authentication reuse**:non-reusable authentication, such as one time passwords (sms, soft token, hard token), reusable authentication (traditional passwords). **•Authentication common methods**: MFA, system to system authentication, identity federation, token-based authentication, biometric authentication, session management (handling of the duration and termination of user sessions), risk-based authentication.• **Strong authentication** involves the use of a minimum of 2FA in combinations with an OTP. FIDO attempts to standardize strong authentication.

Adaptative/Risk-based authentication

> •Adapts authentication measures absed on contextual factors such as location, device or behaviour.

Biometric authentication

> •Uses fingerprints, facial recognition, or other biometric data for user identification. •Important considerations: FAR (false acceptance rate), FRR (false rejection rate), privacy and tracking, biometric data sharing, biometric federation. Positive points: universality, uniueness, measurability, performane, acceptability, circumvention. *Check the table on the type of biometric authentication and it's accuracy, invasiveness, acceptability adn throuhput from CIAP.*

Concepts (cont)

Tokens

> •Is a piece of data that represents the authorization grated for a specific action. It's like a house key (digital key): is proof of your authorization to certain resources or actions•**Types:** soft tokens (generated through software applications), hard tokens (generated by physical devices), RFDI (allows the tagging of physical devices; passive vs active tags; can be combined with other authenication factors; privacy and tracking concerns)

Authorization

> •Process of granting or denying access/privilges to a subject (**someone who is authenticated and is now trying to access an object**), based on the authenticated identity and the associated permissions. •After an user has been successfully authenticated, authorization determines what actions or operations that entity is allowed to perform within the system. •Is about permissions and access control (see access control system types such as: LBAC, TCSEC, MAC, RBAC, RAC, ABAC...). Relies in access policies. •It's important to do periodic access reviews and auditing processes.

Adaptative authorization

> •Authorization changes based on posture. •Linked to adaptative authentication. •e.g.: network access control (when someone connects by vpn, the levels of permissions may change

Inherited permissions

> •Used in some forms of access control models. •Permissions can be inherited through toles or hierarchical structures

Privilege granularity

> •Level of detail and precision at whihc access privileges or permission are defined and managed wihin a system. •Involves breaking down access rights into smlaler, more specific ocmponents, allowing **fine-grained acceess control** (e.g.: instead of granting broad read and write access to a DB, fine-grained access control might allow a user to read specific columns or rows of data) •Traditionl access models lack granularity: you either have access or not. Granular access models are more flexible, you have individual levels of access.

Conditional access policies

> •Allow organization to define access rules based on specific conditions, such as location, device type, or time of the day. e.g.: deny access if the user is trying to log in from an unrecognized or high-risk location.

Delegation of authority

> •Allows adminsitrators or users to grant limited access rights to others without disclosing sensitive information. e.g.: manager delegates authority to approve certain requests without giving full administratve access

Data visibility

> • Different from data accessibility! • Granular access: read, write, list/enumerate,... • Approaches: data hiding and encapsulation; process and memory isolation; interface customisation.n

Access control system types

> •Three party model: subject requests to read/enuerate/write/delete/etc an object (requestor + action + object). If any transaction manages to avoid this process, the IAM is compromised. There's transaction level enforcement of authorization and access policies. •Traditional vs granular access models. •**Types:**LBAC (Label-based access control), TCSEC (trusted computer system evaluation criteria; replaced by Common Criteria [ISO 15408]), MAC (mandatory access control), DAC (discretionary access control), RBAC (role-based access control), RAC (rule based access control), ABAC (attribute based access cotnrol).

Accountability

> End goal of identification, authentication an authorization efforts! Requires uniqueness, defining the accountability scope, protecting accountability data (log retention, capability to remove logs, log timestamp, preserving log integraty, securing logging confidentiality).

Concepts (cont)

SSO (Single Sign On)

> Use of a **single credential** to access multiple systems. • Considerations: if there will be a user repository, where is it going to be? Where is going to be the ultimate identit provider?Which applications that we have support this? If we have low security interfaces maybe we don't extend SSO to them, or we eplace/update them, trusting another system, privacy and tracking. •Not every system will be able to support SSO, butmost modern systems will support APIs orpre-built connectores. • Adv: less credentiasl to manage = - costs, + user capability. Disd: keys to the kigdom, latency risks, strong authentication for trivial access, connectivit issues, resilience, integration complexity.

FIM (Federation Identity Management)

> Use of a **single credential** to access multiple systems. Usually across multiple security domains. • One set of credentials & no need for separate accounts! • Involves identity providers, service providers and trust relationship between them, establlished by standards such as SAML or OAuth. • The line between FIM and SSO is blurry, but they adress different aspects of user authentication and access control: FIM is the same set of credentials to access different resources across multiple domains while SSO is a mechanism thta allows a user to log in once and gain access to multiple applications without having to log in again. Scope: SSO focuses on providing seamless login experience within a single organizaiton or domain and FIM extends the concept to enable users to access resources across different organizations or domains. Authenticaiton model: SSO centralizes authntication within a single domain;FIM allows athentication across federated domains. Use acses: SSO commonly used within a single organization's ecosystem and FIM iwhen users from different organizations need to collaborat and access shared documents. Both rely on standards. Fim often involves the implementation of SSO as part of its broader framework. • Considerations: trusting another system, multiple secrity domaisn, business logic: if someone updates their phonenumber in the intranet phonebook and in the hr system with a different number which will win out? Which direction will the info flow go?, 3rd party Idp, network architecture. • Adv:fewer credentials to manage, customer/supplier integration, policy enforcement. Disd: keys to the kingdom, internet based systems, integration complexity.

Access Control Systems Types

TCSEC	Trusted computer system evaluation	Was replaced by Common Criteria (ISO 15408). •DAC • MAC
MAC	Mandatory access control	Strictest of all models. Difficult to mantain in complex environments due to constant changes. •System controls access. • Subjects
DAC	Discretionary acces control	Resource owner confers access (it's up to thier judgement). More flexible, but challenging in large scale. • NTFS files system
LBAC	Label based access control	Assigns labels to both te subject and the objects based on certain security attributes. Access decisions are then mde by comparing the labels of subjects with the labels of the objects (lists the subject on one side, the object on the other and you plot using a matrix for comparison). Simple approach. • subjects cross referenced to objects. • grid or lattice.

Access Control Systems Types (cont)

RBAC	Role based access control	Assigns permissions to users based on their roles. Associates users with predefined roles and then grants permissions to those roles. Widely used. •Works well where multiple instances of roles exist, but environments with a high number of roles might become complex.
RAC	Rule based access model	Rules define access (access decisions are made by evaluating rules or policies that aredefined and enforced by the system.). Allows fine-grained access control by specifuing conditions or criteria that must be satisfied for access to be granted. • Central management of all rules.
ABAC	Attribute based access control	Determines access based on attributes associated with users, resources and the enviroment. Flexible. • Policy based access control • Strongly relates to XACML standard • User attributtes such as roles, department, location, clearance level... Resource attributs such as sensitivity level, data classification, type...
HBAC	History based access control	Considers the user's historical behaviour (past actions and behaviour patterns) to determinecurrent access permissions.
RiskBAC	Risk based access control	Assesses the risk associated with a particular access request before granting or denying access. Considers factors such as user behaviour, location, and the sensitivity of the requested resource.
TBAC	Temporal based access control	Restricts access based on secific time intervals or temporal conditions. • Time-based policies, such as granting access only during business hours.
HABAC	Hierarchical attribute based access control	Extends ABAC by introducing a hierarchical structure to attributes. Allows for more complex access control policies based on the hierarchical relationships between attributes.
CUI	Contrained user interface	Restricts the functionality or user interface elements available to a user based on their access permissions. •Often used to limit actions within an application

Access Control Systems Types (cont)

UCON	Usage control	Integrates access cotnrol decisions with ongoin usage monitoring. Allows dynameic changes to access permissions based on the user's behaviour during the course of interaction with the system
P2PAC	Peer to peer access control	Enables access control decisions in peer to peer networks. It defines how access permissions are determined in decentralized and distributed systems

IAM Processes

Process approval

> • Designated approver(s) - some processes may require multiple approvers. • Latency vs Security. • Manual vs Automated. • Bulk approval

Monitoring

> • What do we check? How do we check? • Do we perform sample checks (request vs actual), monitor all of the requests in detail or something else? *This might depend on the type of account. Privilege users we might want to monitor more* • What will be the frequency of checks? *This should be linked to the privileges and the risk* • Vulnerability assessment

Review

> Reviwes often refer to the checkign of the request.

Access reviews

> Are necessary! • Who?What?When?How? • point in time assessment • sample checking • check for dormanr accounts, who is using what, privilege users... • management confirmation and review

Reporting

> • What? To whom? How often? • sanitize sensitive info

Credential selection

> Process for selecting appropriate credentials. • username • physical • logial

Credential Issuance

> • Secure channel of issuance • do we need in person verification? • single or multi channel if issuance? • are additional enrolment requirements, such as biometrics, needed? • Considerations: speed vs costs vs security

Provisioning process

> Activities and workflow involved in managing the lifecycle of users. Includes the **user onboarding** (creation and configuration of users accounts), **account modification** (updates to reflect changes on roles, responsabilities or attributes). • Everything should be auditable! • there's a need to understand the scope and the scale required • scripting and automation mght be useful • Considerations: duration of access, account cloning, cross system standardization.

Self service

> Improve the user experince and reduce costs by giving users their own tools to manage IAM. Involves self-service password reset, SSO to access, request and approval, device enrollment, profile management,... •Makes provision faster •

IAM Processes (cont)

Managing change

> Managin changes such as when people move in the organization and permissions have to change. • Do we need to revoke already exiting accesses before giving more privileges? • Processes for exigent ciscumstances like suspension or revocation are needed since the revoke needs to be done instantly.

Deprovisioning

> Activities and workflow needed to manage the **end of a user's lifecycle**. Includes a series of actions to deactivate, delete or transition accounts when an individual leaves the organizaiton or no longer requires specific access or privilege. Includes **user offboarding** (deactivating or deleting user accounts when individuals leave an organization), **account deactivation** (temporarily disabling user accounts in cases such as leaves of absence), **revoking access** (removing access rights and roles), **data archiving or transfer** . • What's the trigger (management notification, removal from the hr systems, lack of activity...) • Needs to be auditable! • How are wegoing to manage everything from access to service accounts to door codes and router passwords? • Sometames disablign an user first and then deprovisioning is better • PII is very important, as well as thinhs like emails on the mailbox • documents that need passwords should also be taken into consideration

IAM processes in an organization can be solely manual or/and have some degree of automation. Example: there can be an manually reviewd pre approval area for accounts thta has been automatically provisioned.

Standards and Guidelines

ISO 27001

> • 14 control domains: A.9 relates to **access management** (access control, access control policy, access to network and network services, user access management which includes provision, PAM, adjustment of access rights, review of access rights... Also coevrs the responsabilities of the user. Considers systems and application access control.

ISO/IEC 24760

> •A framework for **identity management**. • Part 1: terminology and concepts. Considers key processes and terms. Recognized identity and Partial identity (identity distributted over dif. partners that collectivly form an identity). Identifies the lifecycle of an identity (unknown- no degree of trust or evidence-, established, active, suspended, archived). • Part 2: referencearchitecture and requirements for the implementation of idendity management. Includes key terms like relying part, ITP, etc. Recognizes the importance of stakeholders, the use of use cases and ongoing audits. • Part 3: practice. The practical way to comply with the first 2 parts of the standards. Links to **ISO 29003** for proofing (identity proofing) and **ISO 29115** for assurance levels.

NIST SP800-63

> •EUA•Digital identity guidelines • 800-63-3: digital authentication guideline overview • 800-63A: enrolment and identity proofing • 800-63B: authentication and lifecycle management • 800-63C: federation and assertions. • Knowledge based authentication. Covers things like minimum passwords lengths, comparing newpasswords to a dictionary... Recommenrds authoband authentication to provide 2FA, so using separate channels. States that SMS is deprecated for autothanand authenticatio.

National Strategy for Trustd Identities in Syberspace

> •EUA, 2011• Attempt to create trust and a standardized identity on the interet. Privacy, secure, interoprable, cost effectve.

NIST Cybersecurty Practice Gide 1800-2

> •EUA •IAM for electric utilities

NGBMS

> • Research for Next generation measurements and standards for identity management

Standards and Guidelines (cont)

Export of cryptography

> • Different countries have different approaches. Typically there are restrictions on the export of strong cryptography.

Data laws

> • EU= GDPR, EU-US Privacy shield,

Some trends: Russia - data localisation law, South Africa - protection of personal information, Privacy legislation - austria and New Zealanf in 1993 and Honk Kong in 1995, APEC Privacy framework - directive for pacific countiries, China in 2021 -non bidin, focus on protectiong nation. There's a trend to increase regulation regarding data privacy.

Standards and Guidelines

ISO 27001

> • 14 control domains: A.9 relates to **access management** (access control, access control policy, access to network and network services, user access management which includes provision, PAM, adjustment of access rights, review of access rights... Also coevrs the responsabilities of the user. Considers systems and application access control.

ISO/IEC 24760

> •A framework for **identity management**. • Part 1: terminology and concepts. Considers key processes and terms. Recognized identity and Partial identity (identity distributted over dif. partners that collectivly form an identity). Identifies the lifecycle of an identity (unknown- no degree of trust or evidence-, established, active, suspended, archived). • Part 2: referencearchitecture and requirements for the implementation of idendity management. Includes key terms like relying part, ITP, etc. Recognizes the importance of stakeholders, the use of use cases and ongoing audits. • Part 3: practice. The practical way to comply with the first 2 parts of the standards. Links to **ISO 29003** for proofing (identity proofing) and **ISO 29115** for assurance levels.

NIST SP800-63

> •EUA•Digital identity guidelines • 800-63-3: digital authentication guideline overview • 800-63A: enrolment and identity proofing • 800-63B: authentication and lifecycle management • 800-63C: federation and assertions. • Knowledge based authentication. Covers things like minimum passwords lengths, comparing newpasswords to a dictionary... Recommenrds authoband authentication to provide 2FA, so using separate channels. States that SMS is deprecated for autothanand authenticatio.

National Strategy for Trustd Identities in Syberspace

> •EUA, 2011• Attempt to create trust and a standardized identity on the interet. Privacy, secure, interoprable, cost effectve.

NIST Cybersecurty Practice Gide 1800-2

> •EUA •IAM for electric utilities

NGBMS

> • Research for Next generation measurements and standards for identity management

Export of cryptography

> • Different countries have different approaches. Typically there are restrictions on the export of strong cryptography.

Data laws

> • EU= GDPR, EU-US Privacy shield,

Some trends: Russia - data localisation law, South Africa - protection of personal information, Privacy legislation - austria and New Zealanf in 1993 and Honk Kong in 1995, APEC Privacy framework - directive for pacific countiries, China in 2021 -non bidin, focus on protectiong nation. There's a trend to increase regulation regarding data privacy.

Standards and Guidelines

ISO 27001

> • 14 control domains: A.9 relates to **access management** (access control, access control policy, access to network and network services, user access management which includes provision, PAM, adjustment of access rights, review of access rights... Also coevrs the responsabilities of the user. Considers systems and application access control.

ISO/IEC 24760

> •A framework for **identity management**. • Part 1: terminology and concepts. Considers key processes and terms. Recognized identity and Partial identity (identity distributted over dif. partners that collectivly form an identity). Identifies the lifecycle of an identity (unknown- no degree of trust or evidence-, established, active, suspended, archived). • Part 2: referencearchitecture and requirements for the implementation of idendity management. Includes key terms like relying part, ITP, etc. Recognizes the importance of stakeholders, the use of use cases and ongoing audits. • Part 3: practice. The practical way to comply with the first 2 parts of the standards. Links to **ISO 29003** for proofing (identity proofing) and **ISO 29115** for assurance levels.

NIST SP800-63

> •EUA•Digital identity guidelines • 800-63-3: digital authentication guideline overview • 800-63A: enrolment and identity proofing • 800-63B: authentication and lifecycle management • 800-63C: federation and assertions. • Knowledge based authentication. Covers things like minimum passwords lengths, comparing newpasswords to a dictionary... Recommenrds authoband authentication to provide 2FA, so using separate channels. States that SMS is deprecated for autothanand authenticatio.

National Strategy for Trustd Identities in Syberspace

> •EUA, 2011• Attempt to create trust and a standardized identity on the interet. Privacy, secure, interoprable, cost effectve.

NIST Cybersecurty Practice Gide 1800-2

> •EUA •IAM for electric utilities

NGBMS

> • Research for Next generation measurements and standards for identity management

Export of cryptography

> • Different countries have different approaches. Typically there are restrictions on the export of strong cryptography.

Data laws

> • EU= GDPR, EU-US Privacy shield,

Some trends: Russia - data localisation law, South Africa - protection of personal information, Privacy legislation - austria and New Zealanf in 1993 and Honk Kong in 1995, APEC Privacy framework - directive for pacific countiries, China in 2021 -non bidin, focus on protectiong nation. There's a trend to increase regulation regarding data privacy.

Commons Issues

Privilege creep

> Gradual **accumulation of rights** beyond necessary. • Occurs by employee moving on the organization and gets more privileges without having the old one's removed, by excessive privilege assignement, by accumulation of rights...

Mobile computing trend

> Istead of focusing on the corporate network, now it's about trying to secure all information across a **variety o networks**. Also, IAM stretches across corporate and personal devices.

Presumer devices in the enterprise trend

> Bring your own devices trend creates a prioblem.

Commons Issues (cont)

Rate of change

> BYOD (DLP, MDM); Cloud (BYOC), BYOID (IDaaS)

Asset management

> Mangement of physical assets its easier. Its more difficult when there's cloud services and virtualisation. Information as an asset is also difficult to manage.

Cloud & blockchain

Protocols

Technologies