DEFINITION

access control

Posted by: Margaret Rouse WhatIs.com

Contributor(s): Kathleen Richards and Sharon Shea

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

To secure a facility, organizations use electronic access control systems that rely on user credentials, access card readers, auditing and reports to track employee access to restricted business locations and proprietary areas, such as data centers. Some of these systems incorporate access control panels to restrict entry to rooms and buildings as well as alarms and lockdown capabilities to prevent unauthorized access or operations.

Access control systems perform identification authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors. Multifactor authentication, which requires two or more authentication factors, is often an important part of layered defense to protect access control systems.

These security controls work by identifying an individual or entity, verifying that the person or application is who or what it claims to be, and authorizing the access level and set of actions associated with the username or IP address. Directory services and protocols, including the Local Directory Access Protocol (LDAP) and the Security Assertion Markup Language (SAML), provide access controls for authenticating and authorizing users and entities and enabling them to connect to computer resources, such as distributed applications and web servers.

Organizations use different access control models depending on their compliance requirements and the security levels of information technology they are trying to protect.

Types of access control

The main types of access control are:

- **Mandatory access control (MAC)**: A security model in which access rights are regulated by a central authority based on multiple levels of security. Often used in government and military environments, classifications are assigned to system resources and the operating system or security kernel, grants or denies access to those resource objects based on the information security clearance of the user or device. For example, Security Enhanced Linux is an implementation of MAC on the Linux operating system.
- **Discretionary access control (DAC):** An access control method in which owners or administrators of the protected system, data or resource set the policies defining who or what is authorized to access the resource. Many of these systems enable administrators to limit the propagation of access rights. A common criticism of DAC systems is a lack of centralized control.
- **Role-based access control (RBAC):** A widely used access control mechanism that restricts access to computer resources based on individuals or groups with defined business functions -- executive level, engineer level 1 -- rather than the identities of individual users. The role-based security model relies on a complex structure of role assignments, role authorizations and role permissions developed using role engineering to regulate employee access to systems. RBAC systems can be used to enforce MAC and DAC frameworks.
- **Rule-based access control:** A security model in which the system administrator defines the rules that to govern access to resource objects. Often these rules are based on conditions, such as time of day or location. It is not uncommon to use some form of both rule-based access control and role-based access control to enforce access policies and procedures.
- **Attribute-based access control (ABAC):** A methodology that manages access rights by evaluating a set of rules, policies and relationships using the attributes of users, systems and environmental conditions.

Use of access control

The goal of access control is to minimize the risk of unauthorized access to physical and logical systems. Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential information, such as customer data. Most organizations have infrastructure and procedures that limit access to networks, computer systems, applications, files and sensitive data, such as personally identifiable information and intellectual property.

Access control systems are complex and can be challenging to manage in dynamic IT environments that involve on-premises systems and cloud services. After some high-profile breaches, technology vendors have shifted away from single sign-on systems to unified access management, which offers access controls for on-premises and cloud environments.

Implementing access control

Access control is a process that is integrated into an organization's IT environment. It can involve identity and access management systems. These systems provide access control software, a user database, and management tools for access control policies, auditing and enforcement.

When a user is added to an access management system, system administrators use an automated provisioning system to set up permissions based on access control frameworks, job responsibilities and workflows.

The best practice of "least privilege" restricts access to only resources that an employee requires to perform their immediate job functions.

A common security issue is failure to revoke credentials and access to systems and data when an individual moves into a different job internally or leaves the company.

See also: access control list

This was last updated in September 2018

Continue Reading About access control

- Learn how to identify and prevent access control attacks
- CISSP Domain 5 quiz Types of access control systems
- Learn what network access control systems can do for you
- Understand the challenges of implementing secure cloud access control
- Find out about the NIST's access control policy and implementation guide project

Related Terms

identity and access management (IAM)

Identity and access management (IAM) is a framework of business processes, policies and technologies that facilitates the ... See complete definition

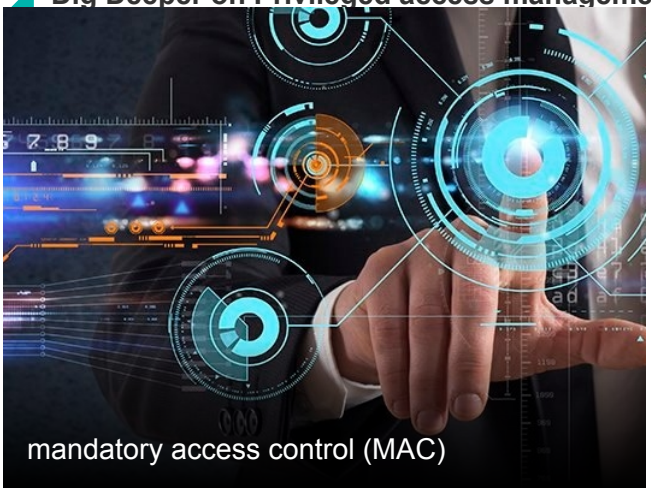
privilege creep

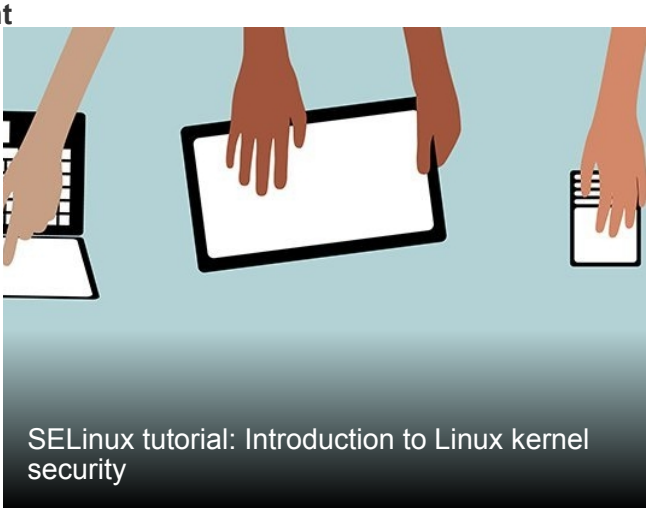
Privilege creep is the gradual accumulation of access rights beyond what an individual needs to do his job. In IT, a privilege is... See complete definition

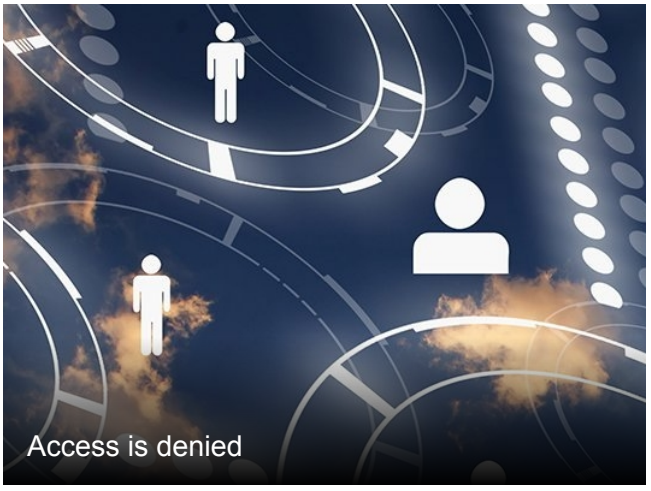
privileged access management (PAM)

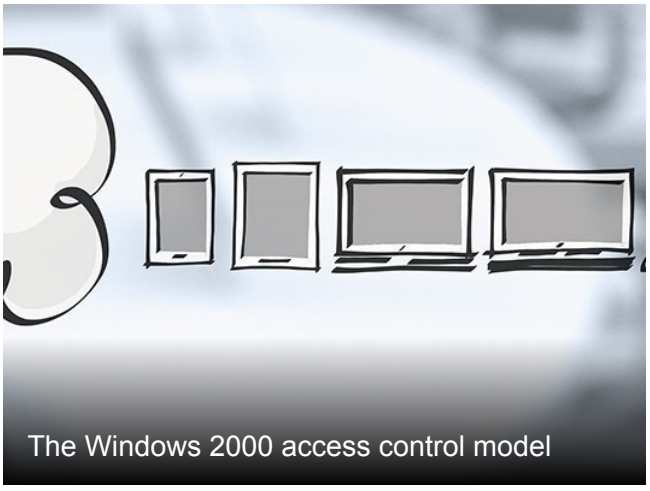
Privileged access management (PAM) is the combination of tools and technology used to secure, control and monitor access to an ...
See complete definition

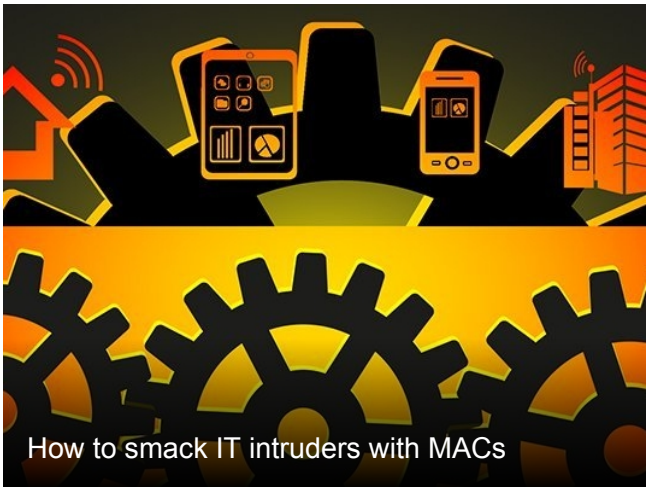
Dig Deeper on Privileged access management











Join the conversation

5 comments

Share your comment

Send me notifications when other members comment.

Add My Comment

Oldest ▼

[-] **Margaret Rouse**

- 30 Jun 2014 9:26 AM

What is the best access control model for cloud computing?

Reply

[-] **securityspark**

- 22 Mar 2017 9:37 AM

well said. You always save my life.

Reply

[-] **MikeMailer**

- 11 Oct 2017 10:34 PM

Was wondering if this is in regards to physical security access control like this definition here: https://www.getkisi.com/access-control

Reply

[-] **secuzose**

- 19 Jul 2019 12:56 AM

What is the best access control model for Complex Enterprise Applications ?

Reply

[-] **marilynstubbs**

- 22 Oct 2019 2:34 PM

How can I recover or change user name and password?

Reply

SearchCloudSecurity

Defining and evaluating SOC as a service

As cloud use increases, many enterprises outsource some security operations center functions. Evaluate if SOCaaS is the best ...

How to beef up S3 bucket security to prevent a breach

Security teams have plenty of tools at their disposal to help their organizations achieve and maintain S3 bucket security. Learn ...