Access control

What is access control?

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.

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

Why is access control important?

The goal of access control is to minimize the security 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 high-profile breaches, technology vendors have shifted away from single sign-on (SSO) systems to unified access management, which offers access controls for on-premises and cloud environments.

How access control works

Access controls identify an individual or entity, verify the person or application is who or what it claims to be, and authorizes the access level and set of actions associated with the username or IP address. Directory services and protocols, including Lightweight Directory Access Protocol and Security Assertion Markup Language, 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 IT they are trying to protect.

4 types of access control
Mandatory access control
Discretionary access control
Rule-based access control
Attribute-based access control
ILLUSTRATION: STONEPIC/ADOBE STOCK; ©2022 TECHTARGET. ALL RIGHTS RESERVED

Types of access control

The main models of access control are the following:

- **Mandatory access control (MAC).** This is 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. MAC grants or denies access to resource objects based on the information security clearance of the user or device. For example, Security-Enhanced Linux is an implementation of MAC on Linux.
- **Discretionary access control (DAC).** This is 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).** This is a widely used access control mechanism that restricts access to computer resources based on individuals or groups with defined business functions -- e.g., executive level, engineer level 1, etc. -- 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.** This is a security model in which the system administrator defines the rules that govern access to resource objects. These rules are often 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 RBAC to enforce access policies and procedures.
- **Attribute-based access control.** This is a methodology that manages access rights by evaluating a set of rules, policies and relationships using the attributes of users, systems and environmental conditions.

Implementing access control

Access control is integrated into an organization's IT environment. It can involve identity management 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 employees require to perform their immediate job functions.

Challenges of access control

Many of the challenges of access control stem from the highly distributed nature of modern IT. It is difficult to keep track of constantly evolving assets because they are spread out both physically and logically. Specific examples of challenges include the following:

Challenges of access control

- Dynamically managing distributed IT environments
- Password fatigue
- Compliance visibility through consistent reporting
- Centralizing user directories and avoiding application-specific silos
- Data governance and reporting

ILLUSTRATION: STONEPIC/ADOBE STOCK; ©2022 TECHTARGET, ALL RIGHTS RESERVED

- dynamically managing distributed IT environments;
- password fatigue;
- compliance visibility through consistent reporting;

- centralizing user directories and avoiding application-specific silos; and
- data governance and visibility through consistent reporting.

Many traditional access control strategies -- which worked well in static environments where a company's computing assets were help on premises -- are ineffective in today's dispersed IT environments.

Modern IT environments consist of multiple cloud-based and hybrid implementations, which spread assets, out over physical locations and over a variety of unique devices, and require dynamic access control strategies.

Organizations often struggle to understand the difference between authentication and authorization: Authentication is the process of verifying individuals are who they say they are using biometric identification and MFA. The distributed nature of assets gives organizations many avenues for authenticating an individual. Authorization is the act of giving individuals the correct data access based on their authenticated identity.

One example of where authorization often falls short is if an individual leaves a job but still has access to that company's assets. This creates security holes because the asset the individual used for work -- a smartphone with company software on it, for example -- is still connected to the company's internal infrastructure but is no longer monitored because the individual is no longer with the company. Left unchecked, this can cause major security problems for an organization. If the ex-employee's device were to be hacked, for example, the attacker could gain access to sensitive company data, change passwords or sell the employee's credentials or the company's data.

One solution to this problem is strict monitoring and reporting on who has access to protected resources so, when a change occurs, it can be immediately identified and access control lists and permissions can be updated to reflect the change.

Another often overlooked challenge of access control is **user experience**. If an access management technology is difficult to use, employees may use it incorrectly or circumvent it entirely, creating security holes and compliance gaps. If a reporting or monitoring application is difficult to use, the reporting may be compromised due to an employee mistake, which would result in a security gap because an important permissions change or security vulnerability went unreported.

Access control software

Many types of access control software and technology exist, and multiple components are often used together as part of a larger identity and access management (IAM) strategy. Software tools may be deployed on premises, in the cloud or both. They may focus primarily on a company's internal access management or outwardly on access management for customers. Types of access management software tools include the following:

- reporting and monitoring applications
- password management tools
- provisioning tools
- identity repositories
- security policy enforcement tools

Microsoft Active Directory is one example of software that includes most of the tools listed above in a single offering. Other IAM vendors with popular products include IBM, Idaptive and Okta.

What is out-of-band authentication?

Out-of-band authentication is a type of two-factor authentication (2FA) that requires a secondary verification method through a separate communication channel along with the typical ID and password. Out-of-band authentication is often used in financial institutions and other organizations with high security requirements.

The fundamental principle behind out-of-band authentication is to introduce an additional layer of security using multiple, unrelated channels. These secondary channels can be a Short Message Service (SMS) text message, a push notification on a mobile device, a voice call or any other means of communication independent of the initial access point. The practice makes hacking an account more difficult because two separate and unconnected authentication channels would need to be compromised for an attacker to gain access.

How does out-of-band authentication work?

The process typically involves the following steps:

- **Initial login.** A user attempts to access a system or application, or tries to perform a sensitive transaction through the primary communication channel, such as a website or mobile app.
- **Secondary verification request.** After the initial login or transaction initiation, the system triggers a request for additional verification through a separate communication channel.
- **Out-of-band delivery.** The system sends a one-time code, also known as a one-time password (OTP), in the form of a push notification or other form of authentication prompt to the user's registered mobile device or different communication channel.
- **User verification.** The user receives the authentication prompt and provides the required information, such as entering the OTP or approving the push notification, through the separate channel.
- **Access granted.** Upon successful verification through both the primary and out-of-band channels, the system grants the user access or completes the requested transaction.

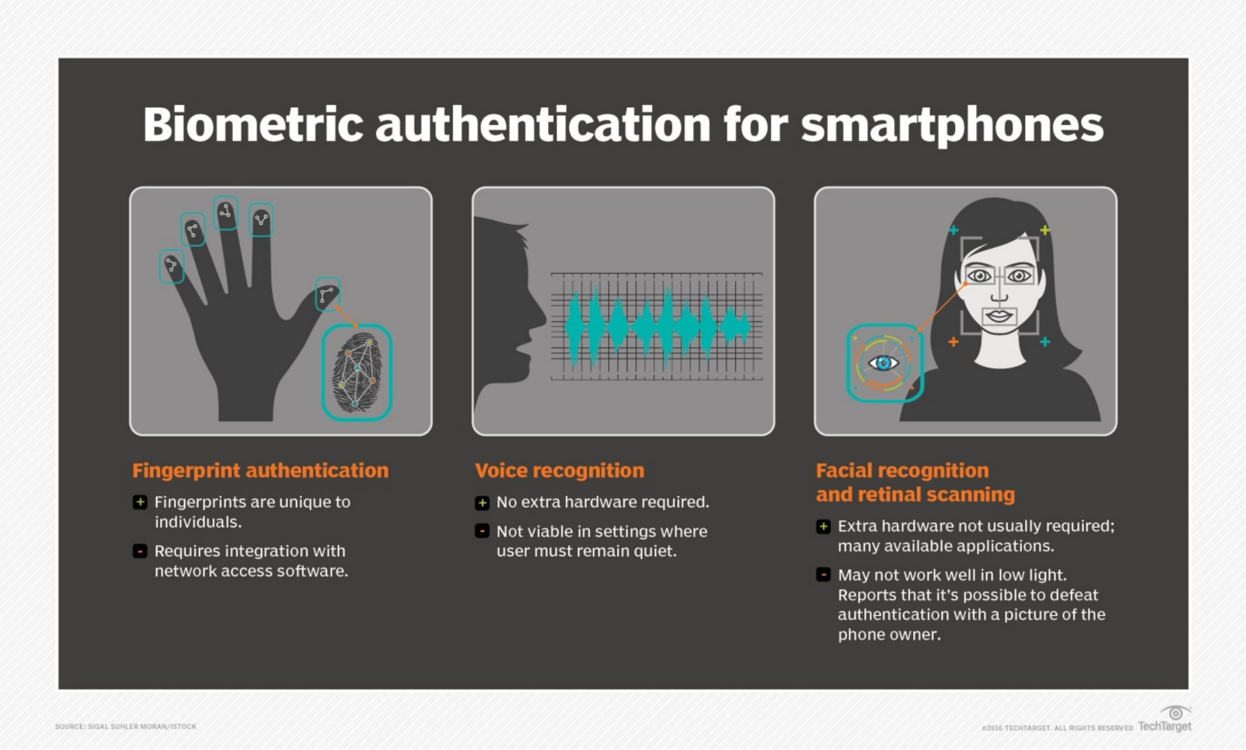
This multichannel approach provides identity and access management functionality that increases the difficulty for attackers to gain unauthorized access. They would need to compromise both the primary and secondary communication channels simultaneously, which is highly improbable.

Examples of out-of-band authentication

Out-of-band authentication can take various forms and apply to different use cases, depending on the specific implementation and the communication channels used. Methods of doing this type of authentication are cheaper to deploy than security key fobs or more complex biometric methods.

Some of the most common examples include the following:

- **SMS one-time passwords.** Users receive a unique, time-sensitive code via SMS on their registered mobile phone, which they must enter to complete the authentication process.
- **Mobile app push notifications.** A dedicated mobile application sends a push notification to the user's device prompting them to approve or deny the login attempt or transaction.
- **Voice calls.** Users must make a phone call from a registered number or respond to an automatically generated phone call from the institution. The system initiates an automated voice call to the user's registered phone number, requiring them to press a specific key or provide a verbal response to confirm their identity. Voice recognition technology can be used to provide biometric verification.
- **Hardware tokens.** Physical devices, such as USB keys and smart cards, generate one-time codes or cryptographic challenges. They serve as an out-of-band authentication factor when used in conjunction with the primary login credentials.
- **Software tokens.** A software token, also known as a soft token, is generated by authenticator apps that provide single-use personal identification numbers (PINs) for authentication. They're made available via applications on computers and mobile devices.
- **Biometric authentication.** Using biometric factors such as voice, fingerprint or facial recognition on a separate device, such as a smartphone, dedicated hardware or security token, can serve as an out-of-band authentication method.



Biometric authentication for smartphones

Fingerprint authentication

- + Fingerprints are unique to individuals.
- - Requires integration with network access software.

Voice recognition

- + No extra hardware required.
- - Not viable in settings where user must remain quiet.

Facial recognition and retinal scanning

- + Extra hardware not usually required; many available applications.
- - May not work well in low light. Reports that it's possible to defeat authentication with a picture of the phone owner.

SOURCE: SIGAL SUHLER MORAN/ISTOCK

©2016 TECHTARGET. ALL RIGHTS RESERVED TechTarget

Who uses out-of-band authentication?

Out-of-band authentication has gained widespread adoption across various industries and sectors because of the strong security capabilities it provides. Industries where it's more likely to be used include the following:

- **Financial services.** Banks, credit card companies and other financial institutions use the technology to secure online transactions, wire transfers and high-value financial operations. It helps prevent fraud and unauthorized access to customer accounts in banking transactions and other financial application.
- **E-commerce and online retailers.** To safeguard sensitive customer information and prevent online banking fraud, e-commerce platforms often incorporate out-of-band authentication during checkout and account management processes.
- **Healthcare.** Medical and other healthcare-related organizations use out-band-authentication to ensure the privacy and security of patient data. It's used to protect electronic health records and sensitive medical information from unauthorized access.
- **Enterprise organizations.** Large companies often implement the technology to secure remote access to corporate networks and proprietary data, as well as to prevent unauthorized access to sensitive systems and applications.

- **Government agencies.** Federal and other government entities handling confidential data such as tax records and classified information rely on out-of-band authentication to enhance data security and protect against cyber attacks and data breaches. Data breaches cost on average $4.45 million U.S., according to IBM's "Cost of a data breach report 2023" conducted by Ponemon Institute.

Top-10 tips for improving cybersecurity

For security professionals

1. Update security policies
2. Require strong authentication for all users
3. Refresh your network security controls
4. Prepare for compromises
5. Keep your security knowledge current
6. Improve employee awareness of security

For employees

7. **Be skeptical.** Always do a sanity check before you open an attachment, click on a link or provide sensitive information.

8. **Be selective.** Use private networks, such as your home network, instead of public networks like the public Wi-Fi at the local coffee shop.

9. **Be organized.** Create a unique strong password for each website and app and use a password manager program that remembers all your passwords.

10. **Be prepared.** Use antimalware software and keep your operating system and applications fully patched. Make sure your data is backed up.

SOURCE: KAREN SCARFONE; ILLUSTRATION: INVINCIBLE_BULLDOG/GETTY IMAGES

©2020 TECHTARGET. ALL RIGHTS RESERVED TechTarget

Strong authentication is considered one of the best methods of improving cyber security.

Benefits and drawbacks of out-of-band authentication

The technology comes with its own set of advantages and potential drawbacks.

Benefits

- **Enhanced security.** By introducing an additional layer of verification through a separate communication channel, out-of-band authentication reduces the risk of successful cyber attacks, such as phishing and man-in-the-middle attacks.

- **Versatility.** The technology can be implemented using various communication channels such as SMS, mobile apps, voice calls and hardware tokens. This lets organizations choose the most suitable method for their users and security requirements.

- **Compliance.** Many regulatory bodies and industry standards mandate the use of multifactor authentication, such as out-of-band authentication.

- **Ease of use.** By using familiar communication channels like mobile devices, this type of authentication technology provides a relatively seamless user experience, eliminating the need to remember complex passwords or carry dedicated hardware tokens.

Drawbacks

- **Threat actors.** Criminals can circumvent out-of-band authentication. For example, a hacker might attempt to substitute their phone number for a customer's on a bank account. In this case, the technology's effectiveness depends on the bank adhering strictly to policies against making changes to an account without phone confirmation or transferring money without that extra authorization.
- **Mobile devices.** Smartphones in particular can be a weak spot in out-of-band-authentication. If people use the same phone for web banking that they use for SMS authentication, they're nullifying the effectiveness of the secondary measure. In either case, the effectiveness of the authentication technology relies upon adherence to the proper procedures.
- **Dependence on communication channels.** The technology relies heavily on the availability and reliability of the communication channels used. Disruptions or delays in these channels can impact the authentication process and user experience.
- **Potential channel vulnerabilities.** Introducing an additional communication channel enhances security but also introduces a new attack surface. Attackers can compromise the out-of-band channel itself by intercepting SMS messages or exploiting vulnerabilities in mobile applications.
- **User adoption challenges.** Users might resist adopting this type of authentication technology because of the perception that it's inconvenient or they aren't familiar with the separate communication channel being used. Proper user education and training are essential for successful implementation.
- **Cost and implementation complexity.** Deploying this sort of authentication technology across an organization can be costly and complex, especially for large-scale implementations. It might require additional infrastructure, integration with existing systems and ongoing maintenance and support.

Other authentication methods

While out-of-band authentication offers strong security, it isn't the only authentication method available. Other types of authentication methods include the following:

    - **Single-factor authentication.** SFA is a traditional method that relies solely on a single factor, such as a password or PIN. Out-of-band authentication provides an extra layer of cyber security by introducing a separate communication channel, making the system or application more resilient against attacks.

    - **Two-factor authentication.** 2FA combines two different authentication factors such as a password and a one-time code sent via SMS or generated by a dedicated app. While 2FA enhances security compared to single-factor authentication, out-of-band authentication goes further, using separate communication channels, reducing the risk of both factors being compromised simultaneously.

Multifactor authentication
Time
Location
Something you have
Something you are
Something you know
55984
*****
ART: MYKYTA/ADOBE STOCK, ALEXDNDZ/ADOBE STOCK
©2022 TECHTARGET. ALL RIGHTS RESERVED.

Out-of-band authentication is a form of multifactor authentication using multiple channels.

- **Multifactor authentication.** MFA involves combining two or more independent authentication factors such as a password, hardware token and a biometric factor. Out-of-band authentication can be considered a form of MFA when implemented using multiple communication channels, providing an additional layer of security beyond traditional MFA implementations.

- **Risk-based authentication.** RBA dynamically adjusts the authentication requirements based on the assessed risk level of a particular login attempt or transaction. Out-of-band authentication can be integrated into a risk-based authentication framework, serving as an additional verification step for high-risk scenarios or transactions deemed potentially fraudulent.

- **What is Multifactor Authentication?**
  See video

  https://www.youtube.com/watch?v=_3rlQVXGKZc

Out-of-band authentication is a popular security and risk management method.