Access control

From Wikipedia, the free encyclopedia

In the fields of physical security and information security, **access control** (**AC**) is the selective restriction of access to a place or other resource[1] while access management describes the process. The act of *accessing* may mean consuming, entering, or using. Permission to access a resource is called *authorization*.

A sailor checks an identification card (ID) before allowing a vehicle to enter a military institution.

Locks and login credentials are two analogous mechanisms of access control.

Contents [hide]

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

In other projects
Wikimedia Commons

Print/export
Create a book
Download as PDF
Printable version

Languages
Deutsch
Español
Français
한국어
हिन्दी
Italiano
Русский
Tiếng Việt
中文
22 more

Edit links

Physical security [edit]

Main article: Physical security

Drop Arm Optical Turnstiles Manufactured by Q-Lane Turnstiles LLc

Geographical access control may be enforced by personnel (e.g., border guard, bouncer, ticket checker), or with a device such as a turnstile. There may be fences to avoid circumventing this access control. An alternative of access control in the strict sense (physically controlling access itself) is a system of checking authorized presence, see e.g. Ticket controller (transportation). A variant is exit control, e.g. of a shop (checkout) or a country.[*citation needed*]

Underground entrance to the New York City Subway system

The term access control refers to the practice of restricting entrance to a property, a building, or a room to authorized persons. Physical access control can be achieved by a human (a guard, bouncer, or receptionist), through mechanical means such as locks and keys, or through technological means such as access control systems like the mantrap. Within these environments, physical key management may also be employed as a means of further managing and monitoring access to mechanically keyed areas or access to certain small assets.[*citation needed*]

Physical access control is a matter of who, where, and when. An access control system determines who is allowed to enter or exit, where they are allowed to exit or enter, and when they are allowed to enter or exit. Historically, this was partially accomplished through keys and locks. When a door is locked, only someone with a key can enter through the door, depending on how the lock is configured. Mechanical locks and keys do not allow restriction of the key holder to specific times or dates. Mechanical locks and keys do not provide records of the key used on any specific door, and the keys can be easily copied or transferred to an unauthorized person. When a mechanical key is lost or the key holder is no longer authorized to use the protected area, the locks must be re-keyed.[2][*citation needed*]

Electronic access control uses computers to solve the limitations of mechanical locks and keys. A wide range of credentials can be used to replace mechanical keys. The electronic access control system grants access based on the credential presented. When access is granted, the door is unlocked for a predetermined time and the transaction is recorded. When access is refused, the door remains locked and the attempted access is recorded. The system will also monitor the door and alarm if the door is forced open or held open too long after being unlocked.[*citation needed*]

Physical security access control with a hand geometry scanner

Access control system operation [edit]

When a credential is presented to a reader, the reader sends the credential's information, usually a number, to a control panel, a highly reliable processor. The control panel compares the credential's number to an access control list, grants or denies the presented request, and sends a transaction log to a database. When access is denied based on the access control list, the door remains locked. If there is a match between the credential and the access control list, the control panel operates a relay that in turn unlocks the door. The control panel also ignores a door open signal to prevent an alarm. Often the reader provides feedback, such as a flashing red LED for an access denied and a flashing green LED for an access granted.[*citation needed*]

Example of fob based access control using an ACT reader

The above description illustrates a single factor transaction. Credentials can be passed around, thus subverting the access control list. For example, Alice has access rights to the server room, but Bob does not. Alice either gives Bob her credential, or Bob takes it; he now has access to the server room. To prevent this, two-factor authentication can be used. In a two factor transaction, the presented credential and a second factor are needed for access to be granted; another factor can be a PIN, a second credential, operator intervention, or a biometric input.[*citation needed*]

There are three types (factors) of authenticating information:[3]

- something the user knows, e.g. a password, pass-phrase or PIN
- something the user has, such as smart card or a key fob
- something the user is, such as fingerprint, verified by biometric measurement

Passwords are a common means of verifying a user's identity before access is given to information systems. In addition, a fourth factor of authentication is now

recognized: someone you know, whereby another person who knows you can provide a human element of authentication in situations where systems have been set up to allow for such scenarios. For example, a user may have their password, but have forgotten their smart card. In such a scenario, if the user is known to designated cohorts, the cohorts may provide their smart card and password, in combination with the extant factor of the user in question, and thus provide two factors for the user with the missing credential, giving three factors overall to allow access.[*citation needed*]

Credential [edit]

A credential is a physical/tangible object, a piece of knowledge, or a facet of a person's physical being that enables an individual access to a given physical facility or computer-based information system. Typically, credentials can be something a person knows (such as a number or PIN), something they have (such as an access badge), something they are (such as a biometric feature), or some combination of these items. This is known as multi-factor authentication. The typical credential is an access card or key-fob, and newer software can also turn users' smartphones into access devices.[4]

There are many card technologies including magnetic stripe, bar code, Wiegand, 125 kHz proximity, 26-bit card-swipe, contact smart cards, and contactless smart cards. Also available are key-fobs, which are more compact than ID cards, and attach to a key ring. Biometric technologies include fingerprint, facial recognition, iris recognition, retinal scan, voice, and hand geometry. The built-in biometric technologies found on newer smartphones can also be used as credentials in conjunction with access software running on mobile devices.[5] In addition to older more traditional card access technologies, newer technologies such as Near field communication (NFC) and Bluetooth low energy can also communicate user credentials to readers for system or building access.[6][7][8]

Access control system components [edit]


Various control system components

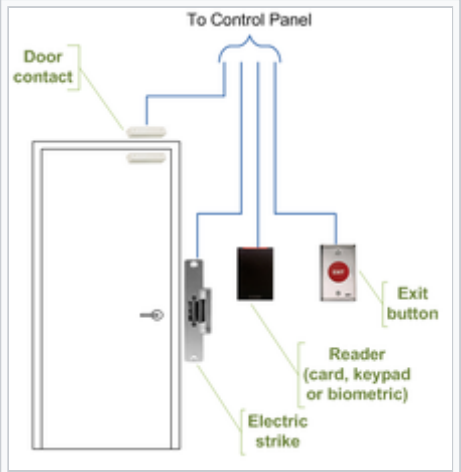
Components of an access control system include:

- An access control panel (also known as a controller)
- An access-controlled entry, such as a door, turnstile, parking gate, elevator, or other physical barrier
- A reader installed near the entry. (In cases where the exit is also controlled, a second reader is used on the opposite side of the entry.)
- Locking hardware, such as electric door strikes and electromagnetic locks
- A magnetic door switch for monitoring door position
- Request-to-exit (REX) devices for allowing egress. When a REX button is pushed, or the motion detector detects motion at the door, the door alarm is temporarily ignored while the door is opened. Exiting a door without having to electrically unlock the door is called mechanical free egress. This is an important

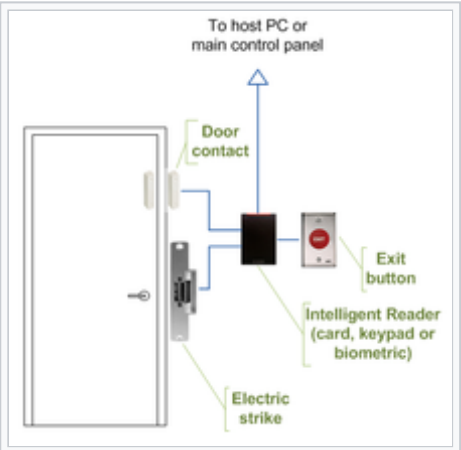
safety feature. In cases where the lock must be electrically unlocked on exit, the request-to-exit device also unlocks the door.[9]

Access control topology [edit]

Access control decisions are made by comparing the credential to an access control list. This look-up can be done by a host or server, by an access control panel, or by a reader. The development of access control systems has seen a steady push of the look-up out from a central host to the edge of the system, or the reader. The predominant topology circa 2009 is hub and spoke with a control panel as the hub, and the readers as the spokes. The look-up and control functions are by the control panel. The spokes communicate through a serial connection; usually RS-485. Some manufactures are pushing the decision making to the edge by placing a controller at the door. The controllers are IP enabled, and connect to a host and database using standard networks[10]



Typical access control door wiring



Access control door wiring when using intelligent readers

Types of readers [edit]

Access control readers may be classified by the functions they are able to perform:[11]

- Basic (non-intelligent) readers: simply read card number or PIN, and forward it to a control panel. In case of biometric identification, such readers output the ID number of a user. Typically, Wiegand protocol is used for transmitting data to the control panel, but other options such as RS-232, RS-485 and Clock/Data are not uncommon. This is the most popular type of access control readers. Examples of such readers are RF Tiny by RFLOGICS, ProxPoint by HID, and P300 by Farpointe Data.
- Semi-intelligent readers: have all inputs and outputs necessary to control door hardware (lock, door contact, exit button), but do not make any access decisions. When a user presents a card or enters a PIN, the reader sends information to the main controller, and waits for its response. If the connection to the main controller is interrupted, such readers stop working, or function in a degraded mode. Usually semi-intelligent readers are connected to a control panel via an RS-485 bus. Examples of such readers are InfoProx Lite IPL200 by CEM Systems, and AP-510 by Apollo.
- Intelligent readers: have all inputs and outputs necessary to control door hardware; they also have memory and processing power necessary to make access decisions independently. Like semi-intelligent readers, they are

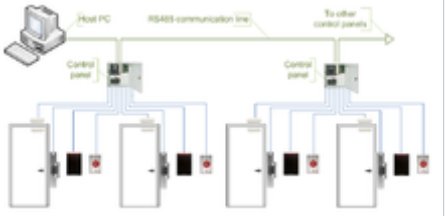
connected to a control panel via an RS-485 bus. The control panel sends configuration updates, and retrieves events from the readers. Examples of such readers could be InfoProx IPO200 by CEM Systems, and AP-500 by Apollo. There is also a new generation of intelligent readers referred to as "IP readers". Systems with IP readers usually do not have traditional control panels, and readers communicate directly to a PC that acts as a host.

Some readers may have additional features such as an LCD and function buttons for data collection purposes (i.e. clock-in/clock-out events for attendance reports), camera/speaker/microphone for intercom, and smart card read/write support.[*citation needed*]

Access control readers may also be classified by their type of identification technology.[*citation needed*]

Access control system topologies [edit]

1. Serial controllers. Controllers are connected to a host PC via a serial RS-485 communication line (or via 20mA current loop in some older systems). External RS-232/485 converters or internal RS-485 cards have to be installed, as standard PCs do not have RS-485 communication ports.[*citation needed*]



Access control system using serial controllers

Advantages:[*citation needed*]

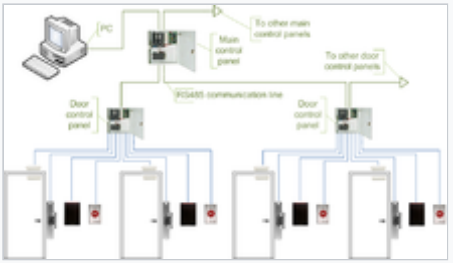
- RS-485 standard allows long cable runs, up to 4000 feet (1200 m)
- Relatively short response time. The maximum number of devices on an RS-485 line is limited to 32, which means that the host can frequently request status updates from each device, and display events almost in real time.
- High reliability and security as the communication line is not shared with any other systems.

Disadvantages:[*citation needed*]

- RS-485 does not allow Star-type wiring unless splitters are used
- RS-485 is not well suited for transferring large amounts of data (i.e. configuration and users). The highest possible throughput is 115.2 kbit/sec, but in most system it is downgraded to 56.2 kbit/sec, or less, to increase reliability.
- RS-485 does not allow the host PC to communicate with several controllers connected to the same port simultaneously. Therefore, in large systems, transfers of configuration, and users to controllers may take a very long time, interfering with normal operations.
- Controllers cannot initiate communication in case of an alarm. The host PC acts as a master on the RS-485 communication line, and controllers have to wait until they are polled.
- Special serial switches are required, in order to build a redundant host PC setup.
- Separate RS-485 lines have to be installed, instead of using an already existing network infrastructure.

- Cable that meets RS-485 standards is significantly more expensive than regular Category 5 UTP network cable.
- Operation of the system is highly dependent on the host PC. In the case that the host PC fails, events from controllers are not retrieved, and functions that require interaction between controllers (i.e. anti-passback) stop working.

2. Serial main and sub-controllers. All door hardware is connected to sub-controllers (a.k.a. door controllers or door interfaces). Sub-controllers usually do not make access decisions, and instead forward all requests to the main controllers. Main controllers usually support from 16 to 32 sub-controllers.



Access control system using serial main and sub-controllers

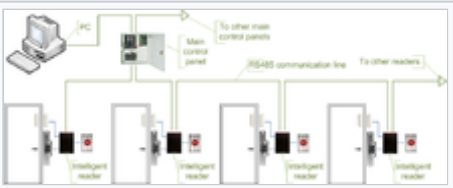
Advantages:[*citation needed*]

- Work load on the host PC is significantly reduced, because it only needs to communicate with a few main controllers.
- The overall cost of the system is lower, as sub-controllers are usually simple and inexpensive devices.
- All other advantages listed in the first paragraph apply.

Disadvantages:[*citation needed*]

- Operation of the system is highly dependent on main controllers. In case one of the main controllers fails, events from its sub-controllers are not retrieved, and functions that require interaction between sub-controllers (i.e. anti-passback) stop working.
- Some models of sub-controllers (usually lower cost) do not have the memory or processing power to make access decisions independently. If the main controller fails, sub-controllers change to degraded mode in which doors are either completely locked or unlocked, and no events are recorded. Such sub-controllers should be avoided, or used only in areas that do not require high security.
- Main controllers tend to be expensive, therefore such a topology is not very well suited for systems with multiple remote locations that have only a few doors.
- All other RS-485-related disadvantages listed in the first paragraph apply.

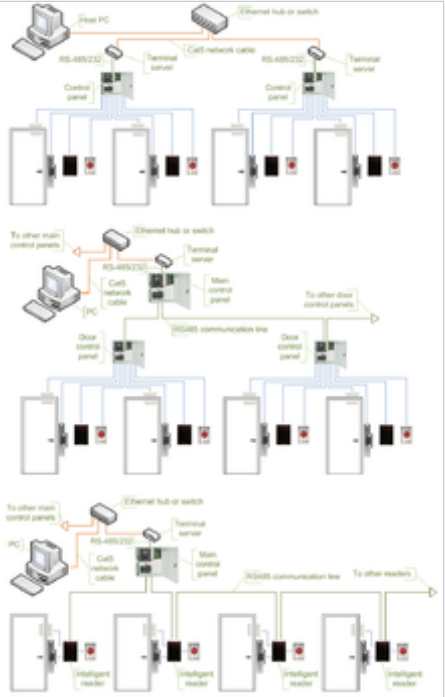
3. Serial main controllers & intelligent readers. All door hardware is connected directly to intelligent or semi-intelligent readers. Readers usually do not make access decisions, and forward all requests to the main controller. Only if the connection to the main controller is unavailable, will the readers use their internal database to make access decisions and record events. Semi-intelligent reader that have no database and cannot function without the main controller should be used only in areas that do not require high security. Main controllers usually support from 16 to 64 readers. All



Access control system using serial main controller and intelligent readers

advantages and disadvantages are the same as the ones listed in the second paragraph.

4. Serial controllers with terminal servers. In spite of the rapid development and increasing use of computer networks, access control manufacturers remained conservative, and did not rush to introduce network-enabled products. When pressed for solutions with network connectivity, many chose the option requiring less efforts: addition of a terminal server, a device that converts serial data for transmission via LAN or WAN.



Access control systems using serial controllers and terminal servers

Advantages:[*citation needed*]

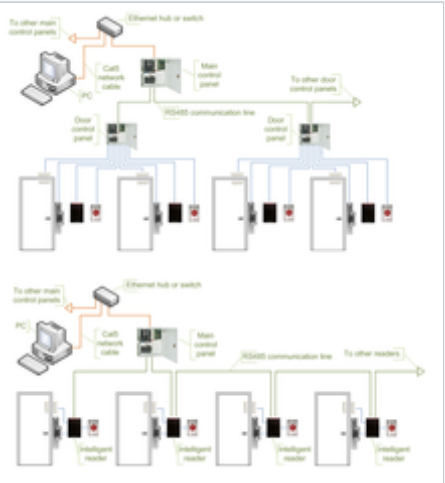
- Allows utilizing the existing network infrastructure for connecting separate segments of the system.
- Provides a convenient solution in cases when the installation of an RS-485 line would be difficult or impossible.

Disadvantages:[*citation needed*]

- Increases complexity of the system.
- Creates additional work for installers: usually terminal servers have to be configured independently, and not through the interface of the access control software.
- Serial communication link between the controller and the terminal server acts as a bottleneck: even though the data between the host PC and the terminal server travels at the 10/100/1000Mbit/sec network speed, it must slow down to the serial speed of 112.5 kbit/sec or less. There are also additional delays introduced in the process of conversion between serial and network data.

All the RS-485-related advantages and disadvantages also apply.

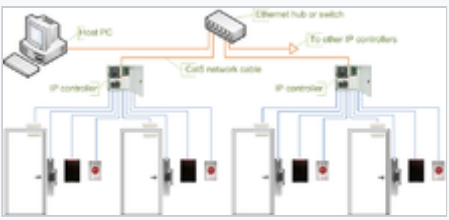
5. Network-enabled main controllers. The topology is nearly the same as described in the second and third paragraphs. The same advantages and disadvantages apply, but the on-board network interface offers a couple of valuable improvements. Transmission of configuration and user data to the main controllers is faster, and may be done in parallel. This makes the system more responsive, and does not interrupt normal operations. No special hardware is required in order to achieve redundant host PC setup: in the case that the primary host



Access control system using network-enabled main controllers

PC fails, the secondary host PC may start polling network controllers. The disadvantages introduced by terminal servers (listed in the fourth paragraph) are also eliminated.

6. IP controllers. Controllers are connected to a host PC via Ethernet LAN or WAN.



Access control system using IP controllers

Advantages:[*citation needed*]

- An existing network infrastructure is fully utilized, and there is no need to install new communication lines.
- There are no limitations regarding the number of controllers (as the 32 per line in cases of RS-485).
- Special RS-485 installation, termination, grounding and troubleshooting knowledge is not required.
- Communication with the controllers may be done at the full network speed, which is important if transferring a lot of data (databases with thousands of users, possibly including biometric records).
- In case of an alarm, controllers may initiate connection to the host PC. This ability is important in large systems, because it serves to reduce network traffic caused by unnecessary polling.
- Simplifies installation of systems consisting of multiple sites that are separated by large distances. A basic Internet link is sufficient to establish connections to the remote locations.
- Wide selection of standard network equipment is available to provide connectivity in various situations (fiber, wireless, VPN, dual path, PoE)

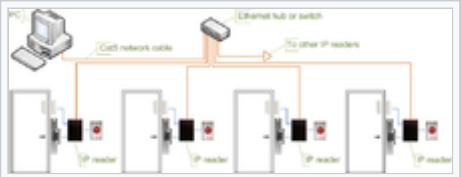
Disadvantages:[*citation needed*]

- The system becomes susceptible to network related problems, such as delays in case of heavy traffic and network equipment failures.
- Access controllers and workstations may become accessible to hackers if the network of the organization is not well protected. This threat may be eliminated by physically separating the access control network from the network of the organization. Most IP controllers utilize either Linux platform or proprietary operating systems, which makes them more difficult to hack. Industry standard data encryption is also used.
- Maximum distance from a hub or a switch to the controller (if using a copper cable) is 100 meters (330 ft).
- Operation of the system is dependent on the host PC. In case the host PC fails, events from controllers are not retrieved and functions that require interaction between controllers (i.e. anti-passback) stop working. Some controllers, however, have a peer-to-peer communication option in order to reduce dependency on the host PC.

7. IP readers. Readers are connected to a host PC via Ethernet LAN or WAN.

Advantages:[*citation needed*]

- Most IP readers are PoE capable. This feature makes it very easy to provide battery backed power to the entire system, including the locks and various types of detectors (if used).
- IP readers eliminate the need for controller enclosures.



Access control system using IP readers

- There is no wasted capacity when using IP readers (e.g. a 4-door controller would have 25% of unused capacity if it was controlling only 3 doors).
- IP reader systems scale easily: there is no need to install new main or sub-controllers.
- Failure of one IP reader does not affect any other readers in the system.

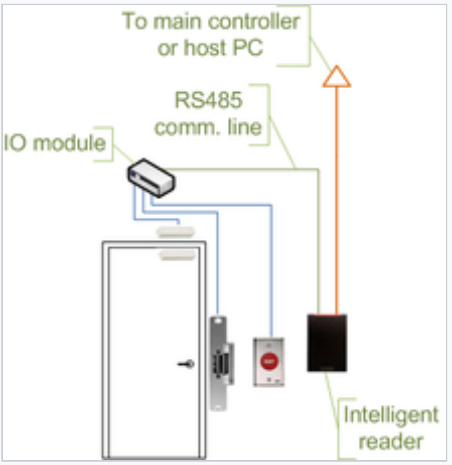
Disadvantages:[*citation needed*]

- In order to be used in high-security areas, IP readers require special input/output modules to eliminate the possibility of intrusion by accessing lock and/or exit button wiring. Not all IP reader manufacturers have such modules available.
- Being more sophisticated than basic readers, IP readers are also more expensive and sensitive, therefore they should not be installed outdoors in areas with harsh weather conditions, or high probability of vandalism, unless specifically designed for exterior installation. A few manufacturers make such models.

The advantages and disadvantages of IP controllers apply to the IP readers as well.

Security risks [edit]

The most common security risk of intrusion through an access control system is by simply following a legitimate user through a door, and this is referred to as tailgating. Often the legitimate user will hold the door for the intruder. This risk can be minimized through security awareness training of the user population or more active means such as turnstiles. In very high-security applications this risk is minimized by using a sally port, sometimes called a security vestibule or mantrap, where operator intervention is required presumably to assure valid identification.[*citation needed*]



Access control door wiring when using intelligent readers and IO module

The second most common risk is from levering a door open. This is relatively difficult on properly secured doors with strikes or high holding force magnetic locks. Fully implemented access control systems include forced door monitoring alarms. These vary in effectiveness, usually failing from high false positive alarms, poor database configuration, or lack of active intrusion monitoring. Most newer access control systems incorporate some type of door prop alarm to inform system administrators of a door left open longer than a specified length of time.[*citation needed*]

The third most common security risk is natural disasters. In order to mitigate risk from natural disasters, the structure of the building, down to the quality of the network and computer equipment vital. From an organizational perspective, the leadership will need to adopt and implement an All Hazards Plan, or Incident Response Plan. The highlights of any incident plan determined by the National Incident Management System must include Pre-incident planning, during incident actions, disaster recovery, and after-action review.[12]

Similar to levering is crashing through cheap partition walls. In shared tenant spaces, the divisional wall is a vulnerability. A vulnerability along the same lines is the breaking of sidelights.[*citation needed*]

Spoofing locking hardware is fairly simple and more elegant than levering. A strong magnet can operate the solenoid controlling bolts in electric locking hardware. Motor locks, more prevalent in Europe than in the US, are also susceptible to this attack using a doughnut-shaped magnet. It is also possible to manipulate the power to the lock either by removing or adding current, although most Access Control systems incorporate battery back-up systems and the locks are almost always located on the secure side of the door.[*citation needed*]

Access cards themselves have proven vulnerable to sophisticated attacks. Enterprising hackers have built portable readers that capture the card number from a user's proximity card. The hacker simply walks by the user, reads the card, and then presents the number to a reader securing the door. This is possible because card numbers are sent in the clear, no encryption being used. To counter this, dual authentication methods, such as a card plus a PIN should always be used.

Many access control credentials unique serial numbers are programmed in sequential order during manufacturing. Known as a sequential attack, if an intruder has a credential once used in the system they can simply increment or decrement the serial number until they find a credential that is currently authorized in the system. Ordering credentials with random unique serial numbers is recommended to counter this threat.[13]

Finally, most electric locking hardware still has mechanical keys as a fail-over. Mechanical key locks are vulnerable to bumping.[14]

The need-to-know principle [edit]

Further information: Principle of least privilege

The need to know principle can be enforced with user access controls and authorization procedures and its objective is to ensure that only authorized individuals gain access to information or systems necessary to undertake their duties.[*citation needed*]

Computer security [edit]

Further information: Computer access control

In computer security, general access control includes authentication, authorization, and audit. A more narrow definition of access control would cover only access approval, whereby the system makes a decision to grant or reject an access request from an already authenticated subject, based on what the subject is authorized to

access. Authentication and access control are often combined into a single operation, so that access is approved based on successful authentication, or based on an anonymous access token. Authentication methods and tokens include passwords, biometric analysis, physical keys, electronic keys and devices, hidden paths, social barriers, and monitoring by humans and automated systems.[*citation needed*]

In any access-control model, the entities that can perform actions on the system are called *subjects*, and the entities representing resources to which access may need to be controlled are called *objects* (see also Access Control Matrix). Subjects and objects should both be considered as software entities, rather than as human users: any human users can only have an effect on the system via the software entities that they control.[*citation needed*]

Although some systems equate subjects with *user IDs*, so that all processes started by a user by default have the same authority, this level of control is not fine-grained enough to satisfy the principle of least privilege, and arguably is responsible for the prevalence of malware in such systems (see computer insecurity).[*citation needed*]

In some models, for example the object-capability model, any software entity can potentially act as both subject and object.[*citation needed*]

As of 2014, access-control models tend to fall into one of two classes: those based on capabilities and those based on access control lists (ACLs).

- In a capability-based model, holding an unforgeable reference or *capability* to an object provides access to the object (roughly analogous to how possession of one's house key grants one access to one's house); access is conveyed to another party by transmitting such a capability over a secure channel
- In an ACL-based model, a subject's access to an object depends on whether its identity appears on a list associated with the object (roughly analogous to how a bouncer at a private party would check an ID to see if a name appears on the guest list); access is conveyed by editing the list. (Different ACL systems have a variety of different conventions regarding who or what is responsible for editing the list and how it is edited.)[*citation needed*]

Both capability-based and ACL-based models have mechanisms to allow access rights to be granted to all members of a *group* of subjects (often the group is itself modeled as a subject).[*citation needed*]

Access control systems provide the essential services of *authorization*, *identification and authentication* (*I&A*), *access approval*, and *accountability* where:[*citation needed*]

- authorization specifies what a subject can do
- identification and authentication ensure that only legitimate subjects can log on to a system
- access approval grants access during operations, by association of users with the resources that they are allowed to access, based on the authorization policy
- accountability identifies what a subject (or all subjects associated with a user) did

Access control models [edit]

Access to accounts can be enforced through many types of controls.[15]

1. Attribute-based Access Control (ABAC)
   An access control paradigm whereby access rights are granted to users through the use of policies which evaluate attributes (user attributes, resource attributes and environment conditions)[16]
2. Discretionary Access Control (DAC)
   In DAC, the data owner determines who can access specific resources. For example, a system administrator may create a hierarchy of files to be accessed based on certain permissions.
3. History-Based Access Control (HBAC)
   Access is granted or declined based on the real-time evaluation of a history of activities of the inquiring party, e.g. behavior, time between requests, content of requests.[17] For example, the access to a certain service or data source can be granted or declined on the personal behavior, e.g. the request interval exceeds one query per second.
4. Identity-Based Access Control (IBAC)
   Using this network administrators can more effectively manage activity and access based on individual needs.[18]
5. Mandatory Access Control (MAC)
   In MAC, users do not have much freedom to determine who has access to their files. For example, security clearance of users and classification of data (as confidential, secret or top secret) are used as security labels to define the level of trust.
6. Organization-Based Access control (OrBAC)
   OrBAC model allows the policy designer to define a security policy independently of the implementation[19]
7. Role-Based Access Control (RBAC)
   RBAC allows access based on the job title. RBAC largely eliminates discretion when providing access to objects. For example, a human resources specialist should not have permissions to create network accounts; this should be a role reserved for network administrators.
8. Rule-Based Access Control (RAC)
   RAC method is largely context based. Example of this would be only allowing students to use the labs during a certain time of day.
9. Responsibility Based Access control
   Information is accessed based on the responsibilities assigned to an actor or a business role[20]

Telecommunication [edit]

In telecommunication, the term *access control* is defined in U.S. Federal Standard 1037C[21] with the following meanings:

1. A service feature or technique used to permit or deny use of the components of a communication system.
2. A technique used to define or restrict the rights of individuals or application programs to obtain data from, or place data onto, a storage device.

3. The definition or restriction of the rights of individuals or application programs to obtain data from, or place data into, a storage device.
4. The process of limiting access to the resources of an AIS (Automated Information System) to authorized users, programs, processes, or other systems.
5. That function performed by the resource controller that allocates system resources to satisfy user requests.

This definition depends on several other technical terms from Federal Standard 1037C.

In object-oriented programming [edit]

In object-oriented programming languages, *access control* is a part of the apparatus of achieving encapsulation, one of four fundamentals of object-oriented programming. The goal is to establish a clear separation between interface (visible and accessible parts of the class) and implementation (internal representation and helper methods).

Also known as data hiding, it ensures exclusive data access to class members (both variables and methods) and protects object integrity by preventing corruption by a client programmer/ client classes. Rule of thumb is to use the more restrictive access level for your data, unless there is a compelling reason to expose it. This also helps to reduce interdependencies between classes - leading to lower coupling and fewer regression bugs.[22]

In object-oriented programming, *access control* is typically implemented using access modifiers in the object or class. Although access modifiers may be syntactically different between languages, they all attempt to achieve the same goal; Define which variables and methods are visible and to whom.

Several programming languages (e.g. Java, C++, C#, Ruby) use the same **public**, **protected** and **private** access modifiers. These are the keywords which allow a programmer to establish access levels to classes and class members (both data and methods). Their exact use in each programming language is varied, depending on the language philosophy, but there are more similarities than differences.[23]

Comparison of use of access modifier keywords in different OOP languages [edit]

Keyword	C++	Java	PHP	Ruby	C#
`private`	class	class	class	-	class
`protected`	derived classes	derived classes *and/or* within same package	derived class	derived classes	derived class
`package`	-	within its package	-	-	-

`internal`	-	-	-	-	current assembly
`public`	everybody	everybody	everybody	everybody	everybody
no modifier (default)	class	same package	everybody	everybody	class

[24] [25]

Note: in Ruby, **private** methods always have **self** as an implicit receiver. Therefore, they can only be used on their current object.

In some languages there are mechanisms to override access modifies to gain access to the private components of an object. One such example is the friend class in C++.

Attribute accessors [edit]

Special public member methods - **accessors** (aka **getters**) and **mutator methods** (often called **setters**) are used to control changes to class variables in order to prevent unauthorized access and data corruption.

Public policy [edit]

In public policy, access control to restrict access to systems ("authorization") or to track or monitor behavior within systems ("accountability") is an implementation feature of using trusted systems for security or social control.

See also [edit]

- Alarm device, Alarm management, Security alarm
- Card reader, Common Access Card, Magnetic stripe card, Proximity card, Smart card, Optical turnstile, Access badge
- Castle, Fortification
- Computer security, Logical security, .htaccess, Wiegand effect, XACML, Credential
- Door security, Lock picking, Lock (security device), Electronic lock, Safe, Safe-cracking, Bank vault
- Fingerprint scanner, Photo identification, Biometrics
- Identity management, Identity document, OpenID, IP Controller, IP reader
- Key management, Key cards
- Lock screen
- Physical security information management
- Physical Security Professional
- Prison, Barbed tape, Mantrap
- Security, Security engineering, Security lighting, Security management, Security policy

References [edit]

1. ^ RFC 4949
2. ^ Niemelä, Harri (2011). "The study of business opportunities and value add of NFC applications in security". *www.theseus.fi*. Retrieved 2019-03-22.
3. ^ Federal Financial Institutions Examination Council (2008). "Authentication in an Internet Banking Environment" (PDF). Archived (PDF) from the original on 2010-05-05. Retrieved 2009-12-31.
4. ^ "MicroStrategy's office of the future includes mobile identity and cybersecurity". *Washington Post*. 2014-04-14. Archived from the original on 2014-02-16. Retrieved 2014-03-30.
5. ^ "iPhone 5S: A Biometrics Turning Point?". BankInfoSecurity.com. 2013-09-16. Archived from the original on 2015-09-11. Retrieved 2014-03-30.
6. ^ "NFC access control: cool and coming, but not close". Security Systems News. 2013-09-25. Archived from the original on 2014-04-06. Retrieved 2014-03-30.
7. ^ "Ditch Those Tacky Key Chains: Easy Access with EC Key". Wireless Design and Development. 2012-06-11. Archived from the original on 2014-04-07. Retrieved 2014-03-31.
8. ^ "Kisi And KeyMe, Two Smart Phone Apps, Might Make House Keys Obsolete". *The Huffington Post*. The Huffington Post. Archived from the original on 11 March 2015. Retrieved 2 September 2015.
9. ^ Rhodes, Brian (2019). "Designing Access Control Guide". *ipvm.com*. Retrieved 2019-10-01.
10. ^ "Opening new doors with IP access control - Secure Insights". *Secure Insights*. 2018-03-16. Retrieved 2018-06-20.
11. ^ "The Evolution of Access Control". *isonas.com*. Retrieved 26 September 2019.
12. ^ "Incident Command System :: NIMS Online :: Serving the National Incident Management System (NIMS) Community". 2007-03-18. Archived from the original on March 18, 2007. Retrieved 2016-03-06.
13. ^ "Smart access control policies for residential & commercial buildings". Archived from the original on 4 July 2017. Retrieved 11 September 2017.
14. ^ Graham Pulford (17 October 2007). *High-Security Mechanical Locks: An Encyclopedic Reference*. Butterworth-Heinemann. pp. 76–. ISBN 978-0-08-055586-7.
15. ^ "Cybersecurity: Access Control". 4 February 2014. Retrieved 11 September 2017.
16. ^ "SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations" (PDF). NIST. 2014. Archived from the original (PDF) on 2016-03-05. Retrieved 2015-12-08.
17. ^ Schapranow, Matthieu-P. (2014). *Real-time Security Extensions for EPCglobal Networks*. Springer. ISBN 978-3-642-36342-9.
18. ^ http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=8,984,620.PN.&OS=PN/8,984,620&RS=PN/8,984,620 [*permanent dead link*]
19. ^ "OrBAC: Organization Based Access Control - The official OrBAC model website". *orbac.org*. Archived from the original on 2017-06-10. Retrieved 11 September 2017.
20. ^ "Archived copy" (PDF). Archived (PDF) from the original on 2016-03-04. Retrieved 2014-07-18.
21. ^ "Archived copy" (PDF). Archived from the original (PDF) on 2007-05-08. Retrieved 2007-01-23.
22. ^ "What is Data Hiding? - Definition from". Archived from the original on 12 September 2017. Retrieved 11 September 2017.

23. ^ "Controlling Access to Members of a Class (The Java™ Tutorials Learning the Java Language > Classes and Objects)". *docs.oracle.com*. Archived from the original on 30 September 2017. Retrieved 11 September 2017.
24. ^ ealigam@gmail.com, Satish Talim / Original design: Erwin Aligam -. "Ruby Access Control: Ruby Study Notes - Best Ruby Guide, Ruby Tutorial". *rubylearning.com*. Archived from the original on 29 June 2017. Retrieved 11 September 2017.
25. ^ "Classes (I) - C++ Tutorials". *www.cplusplus.com*. Archived from the original on 4 January 2018. Retrieved 11 September 2017.

- U.S. Federal 1037C
- U.S. MIL-188
- U.S. National Information Systems Security Glossary
- Harris, Shon, All-in-one CISSP Exam Guide, 6th Edition, McGraw Hill Osborne, Emeryville, California, 2012.
- "Integrated Security Systems Design" - Butterworth/Heinenmann - 2007 - Thomas L. Norman, CPP/PSP/CSC Author
- NIST.gov - Computer Security Division - Computer Security Resource Center - ATTRIBUTE BASED ACCESS CONTROL (ABAC) - OVERVIEW

External links [edit]

- Access Control Markup Language. An OASIS standard language/model for access control. Also XACML.
- Control de acceso (in Spanish)

Wikimedia Commons has media related to ***Access control systems***.

Authority control BNF: cb11973131k (data) · GND: 4293034-0 · LCCN: sh85000357

Categories: Access control | Identity management | Computer security | Perimeter security | Physical security