SOFTWARE CONTROL SERVICES (PTY) LTD

475 King's Highway, Lynnwood
P.O.Box 36675, Menlo Park
Pretoria, South Africa
0102

(t) +27 12 348 7301
(f) +27 12 348 1129
(e) techsupport@softconserv.com
www.softconserv.com

Access control.

Version 0. 1

Prepared by: Michael Davis- Hannibal

Softcon Software Control Services (Pty) Ltd.

7 March 2017

Revision History

Name	Date	Reason For Changes	Version
MDH	28-Jul-10	Initial document	0.1

Contents

General

Access control is a system which enables an authority to control access to areas and resources in a given physical facility or computer-based information system. An access control system, within the field of physical security, is generally seen as the second layer in the security of a physical structure.

Access control is, in reality, an everyday phenomenon. A lock on a car door is essentially a form of access control. A PIN on an ATM system at a bank is another means of access control. Bouncers standing in front of a night club is perhaps a more primitive mode of access control (given the evident lack of information technology involved). The possession of access control is of prime importance when persons seek to secure important, confidential, or sensitive information and equipment.

Item control or electronic key management is an area within (and possibly integrated with) an access control system which concerns the managing of possession and location of small assets or physical (mechanical) keys.

Physical access

Figure 1: Access

Physical access by a person may be allowed depending on payment, authorization, etc. Also there may be one-way traffic of people. These can be enforced by personnel such as a border guard, a doorman, a ticket checker, etc., 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.

In physical security, 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 Access control vestibule. 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.

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.

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.

Access control system operation

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.

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.

There are three types (factors) of authenticating information:

- something the user knows, eg a password, pass-phrase or PIN
- something the user has, such as smart card
- 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, where 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 missing credential, and three factors overall to allow access.

Credential

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 you know (such as number or PIN), something you have (such as an access badge), something you are (such as a biometric feature) or some combination of these items. The typical credential is an access card, key fob, or other key. 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. Typical biometric technologies include fingerprint, facial recognition, iris recognition, retinal scan, voice, and hand geometry.

Access control system components

An access control point, which can be a door, turnstile, parking gate, elevator, or other physical barrier where granting access can be electronically controlled. Typically the access point is a door. An electronic access control door can contain several elements. At its most basic there is a stand-alone electric lock. The lock is unlocked by an operator with a switch. To automate this, operator intervention is replaced by a reader. The reader could be a keypad where a code is entered, it could be a card reader, or it could be a biometric reader. Readers do not usually make an access decision but send a card number to an access control panel that verifies the number against an access list. To monitor the door position a magnetic door switch is used. In concept the door switch is not unlike those on refrigerators or car doors. Generally only entry is controlled and exit is uncontrolled. In cases where exit is also controlled a second reader is used on the opposite side of the door. In cases where exit is not controlled, free exit, a device called a request-to-exit (RTE) is used. Request-to-exit devices can be a pushbutton or a motion detector. When the 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.

Access control topology

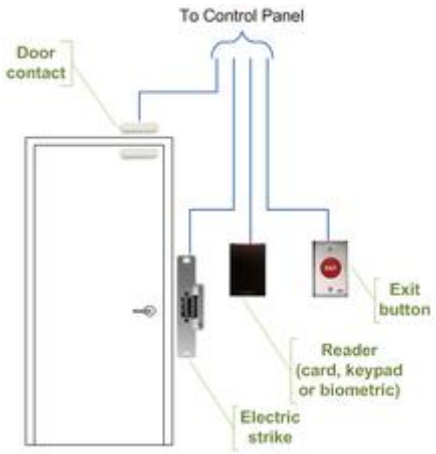

Figure 2: Typical access control door wiring

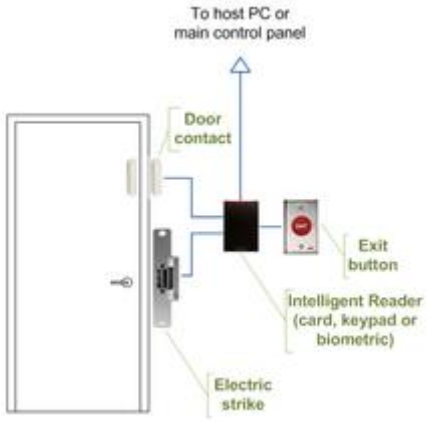

Figure 3: Access control door wiring when using intelligent readers

Access control decisions are made by comparing the credential to an access control list. This lookup 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 lookup out from a central host to the edge of the system, or the reader. The predominate topology circa 2009 is hub and spoke with a control panel as the hub and the readers as the spokes. The lookup and control functions are by the control panel. The spokes communicate through a serial connection; usually RS485. 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.

Types of readers

Access control readers may be classified by functions they are able to perform:

- 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 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 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. Same as 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 PC that acts as a host. Examples of such readers are PowerNet IP Reader by Isonas Security

Systems, ID08 by Solus has the built in webservice to make it user friendly, Edge ER40 reader by HID Global, LogLock and UNiLOCK by ASPiSYS Ltd, and BioEntry Plus reader by Suprema Inc.

Some readers may have additional features such as 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.

Access control readers may also be classified by the type of identification technology.

Access control system topologies

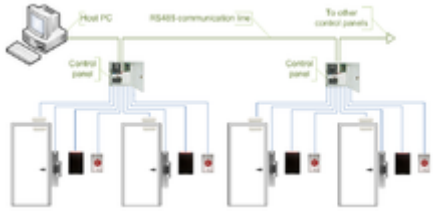

Figure 4: Access control system using serial controllers

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. In larger systems multi-port serial IO boards are used, Digi International being one of most popular options. Advantages:

- 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:

- RS-485 does not allows 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/s, but in most system it is downgraded to 56.2 kbit/s or less to increase reliability.
- RS-485 does not allow 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 and interfere 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 till 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 the regular Category 5 UTP network cable.

- Operation of the system is highly dependent on the host PC. In case the host PC fails, events from controllers are not retrieved and functions that required interaction between controllers (i.e. anti-passback) stop working.

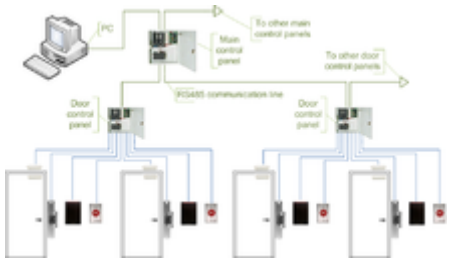

Figure 5:Access control system using serial main and sub-controllers

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 forward all requests to the main controllers. Main controllers usually support from 16 to 32 sub-controllers. Advantages:

- 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:

- 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) have no memory and 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 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.

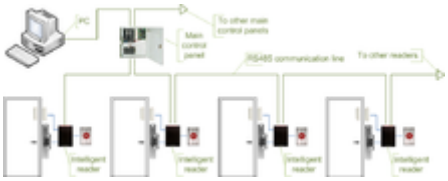

Figure 6: Access control system using serial main controller and intelligent readers

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

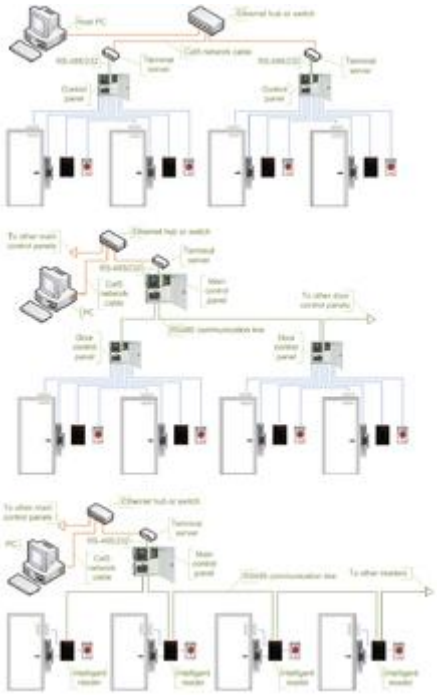

Figure 7: Access control systems using serial controllers and terminal servers

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. Terminal servers manufactured by Lantronix and Tibbo Technology are popular in the security industry. Advantages:

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

Disadvantages:

- Increases complexity of the system.
- Creates additional work for installers: usually terminal servers have to be configured independently, 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/s network speed it then slows down to the serial speed of 112.5 kbit/s or less. There are also additional delays introduced in the process of conversion between serial and network data.

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

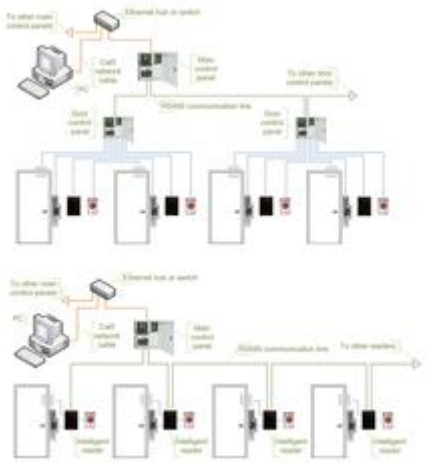

Figure 8: Access control system using network-enabled main controllers

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 valuable improvements. Transmission of configuration and users 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 case the primary host 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.

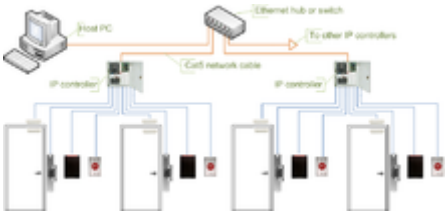

Figure 9: Access control system using IP controllers

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

- An existing network infrastructure is fully utilized, there is no need to install new communication lines.
- There are no limitations regarding the number of controllers (32 per line in case of RS-485).
- Special RS-485 installation, termination, grounding and troubleshooting knowledge is not required.
- Communication with 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 allows to reduce network traffic caused by unnecessary polling.

- Simplifies installation of systems consisting of multiple sites separated by large distances. Basic Internet link is sufficient to establish connections to remote locations.
- Wide selection of standard network equipment is available to provide connectivity in different situations (fiber, wireless, VPN, dual path, PoE)

Disadvantages:

- 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. Also it should be noted that 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 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 required interaction between controllers (i.e. anti-passback) stop working. Some controllers, however, have peer-to-peer communication option in order to reduce dependency on the host PC.

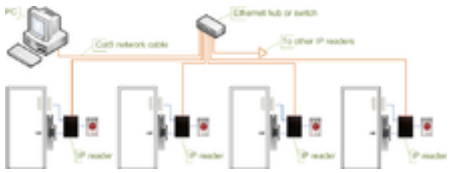

Figure 10: Access control system using IP readers

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

- 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.
- There is no wasted capacity when using IP readers (i.e. a 4-door controller would have 25% 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:

- 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 possibility of vandalism.
- The variety of IP readers in terms of identification technologies and read range is much lower than that of the basic readers.

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

Security risks

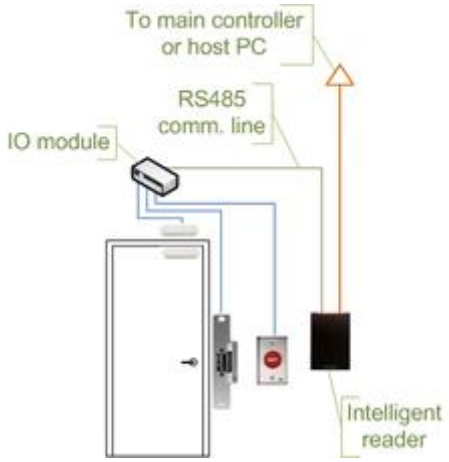

Figure 11: Access control door wiring when using intelligent readers and IO module

The most common security risk of intrusion of an access control system is simply following a legitimate user through a door. 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.

The second most common risk is from levering the door open. This is surprisingly simple and effective on most doors. The lever could be as small as a screw driver or big as a crow bar. 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.

Similar to levering is crashing through cheap partition walls. In shared tenant spaces the demisal wall is a vulnerability. Along the same lines is breaking sidelights.

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 donut shaped magnet. It is also possible to manipulate the power to the lock either by removing or adding current.

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.

Finally, most electric locking hardware still have mechanical keys as a failover. Mechanical key locks are vulnerable to bumping.

The need-to-know principle

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. See Principle_of_least_privilege.

Computer security

In computer security, access control includes authentication, authorization and audit. It also includes measures such as physical devices, including biometric scans and metal locks, hidden paths, digital signatures, encryption, social barriers, and monitoring by humans and automated systems.

In any access control model, the entities that can perform actions in 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 and as human users[1]. 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).

In some models, for example the object-capability model, any software entity can potentially act as both a subject and object.

Access control models used by current systems 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 your house key grants you access to your 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 is on a list associated with the object (roughly analogous to how a bouncer at a private party would check your ID to see if your name is 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.)

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).

Access control systems provide the essential services of *identification and authentication* (*I&A*), *authorization*, and *accountability* where:

- identification and authentication determine who can log on to a system, and the association of users with the software subjects that they are able to control as a result of logging in;
- authorization determines what a subject can do;
- accountability identifies what a subject (or all subjects associated with a user) did.

Identification and authentication (I&A)

Identification and authentication (I&A) is the process of verifying that an identity is bound to the entity that makes an assertion or claim of identity. The I&A process assumes that there was an initial validation of the identity, commonly called identity proofing. Various methods of identity proofing are available ranging from in person validation using government issued identification to anonymous methods that allow the claimant to remain anonymous, but known to the system if they return. The method used for identity proofing and validation should provide an assurance level commensurate with the intended use of the identity within the system. Subsequently, the entity asserts an identity together with an authenticator as a means for validation. The only requirements for the identifier is that it must be unique within its security domain.

Authenticators are commonly based on at least one of the following four factors:

- *Something you know*, such as a password or a personal identification number (PIN). This assumes that only the owner of the account knows the password or PIN needed to access the account.
- *Something you have*, such as a smart card or security token. This assumes that only the owner of the account has the necessary smart card or token needed to unlock the account.
- *Something you are*, such as fingerprint, voice, retina, or iris characteristics.
- *Where you are*, for example inside or outside a company firewall, or proximity of login location to a personal GPS device.

Authorization

Authorization applies to subjects. Authorization determines what a subject can do on the system.

Most modern operating systems define sets of permissions that are variations or extensions of three basic types of access:

- Read (R): The subject can
    - Read file contents
    - List directory contents
- Write (W): The subject can change the contents of a file or directory with the following tasks:
    - Add
    - Create
    - Delete
    - Rename
- Execute (X): If the file is a program, the subject can cause the program to be run. (In Unix systems, the 'execute' permission doubles as a 'traverse directory' permission when granted for a directory.)

These rights and permissions are implemented differently in systems based on *discretionary access control* (*DAC*) and *mandatory access control* (*MAC*).

Accountability

Accountability uses such system components as *audit trails* (records) and *logs* to associate a subject with its actions. The information recorded should be sufficient to map the subject to a controlling user. Audit trails and logs are important for

- Detecting security violations
- Re-creating security incidents

If no one is regularly reviewing your logs and they are not maintained in a secure and consistent manner, they may not be admissible as evidence.

Many systems can generate automated reports based on certain predefined criteria or thresholds, known as *clipping levels*. For example, a clipping level may be set to generate a report for the following:

- More than three failed logon attempts in a given period
- Any attempt to use a disabled user account

These reports help a system administrator or security administrator to more easily identify possible break-in attempts.

Access control techniques

Access control techniques are sometimes categorized as either discretionary or non-discretionary. The three most widely recognized models are Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC). MAC and RBAC are both non-discretionary.

Attribute-based access control

In attribute-based access control (ABAC), access is granted not based on the rights of the subject associated with a user after authentication, but based on attributes of the user. The user has to prove so called claims about his attributes to the access control engine. An attribute-based access control policy specifies which claims need to satisfied in order to grant access to an object. For instance the claim could be "older than 18" . Any user that can prove this claim is granted access. Users can be anonymous as authentication and identification are not strictly required. One does however require means for proving claims anonymously. This can for instance be achieved using anonymous credentials or XACML (extensible access control markup language).

Discretionary access control

Discretionary access control (DAC) is an access policy determined by the owner of an object. The owner decides who is allowed to access the object and what privileges they have.

Two important concepts in DAC are

- File and data ownership: Every object in the system has an *owner*. In most DAC systems, each object's initial owner is the subject that caused it to be created. The access policy for an object is determined by its owner.
- Access rights and permissions: These are the controls that an owner can assign to other subjects for specific resources.

  Access controls may be discretionary in ACL-based or capability-based access control systems. (In capability-based systems, there is usually no explicit concept of 'owner', but the creator of an object has a similar degree of control over its access policy.)

Mandatory access control

Mandatory access control (MAC) is an access policy determined by the system, not the owner. MAC is used in multilevel systems that process highly sensitive data, such as classified government and military information. A multilevel system is a single computer system that handles multiple classification levels between subjects and objects.

- Sensitivity labels: In a MAC-based system, all subjects and objects must have labels assigned to them. A subject's sensitivity label specifies its level of trust. An object's sensitivity label specifies the level of trust required for access. In order to access a given object, the subject must have a sensitivity level equal to or higher than the requested object.
- Data import and export: Controlling the import of information from other systems and export to other systems (including printers) is a critical function of MAC-based systems, which must ensure that sensitivity labels are properly maintained and implemented so that sensitive information is appropriately protected at all times.

  Two methods are commonly used for applying mandatory access control:

- Rule-based (or label-based) access control: This type of control further defines specific conditions for access to a requested object. All MAC-based systems implement a simple form of rule-based access control to determine whether access should be granted or denied by matching:
  - An object's sensitivity label
  - A subject's sensitivity label
- Lattice-based access control: These can be used for complex access control decisions involving multiple objects and/or subjects. A lattice model is a mathematical structure that defines greatest lower-bound and least upper-bound values for a pair of elements, such as a subject and an object.

  Few systems implement MAC; XTS-400 is an example of one that does. The computer system at the company in the movie *Tron* is an example of MAC in popular culture.

Role-based access control

Role-based access control (RBAC) is an access policy determined by the system, not the owner. RBAC is used in commercial applications and also in military systems, where multi-level security requirements may also exist. RBAC differs from DAC in that DAC allows users to control access to their resources, while in RBAC, access is controlled at the system level, outside of the user's control. Although RBAC is non-discretionary, it can be distinguished from MAC primarily in the way permissions are

handled. MAC controls read and write permissions based on a user's clearance level and additional labels. RBAC controls collections of permissions that may include complex operations such as an e-commerce transaction, or may be as simple as read or write. A role in RBAC can be viewed as a set of permissions.

Three primary rules are defined for RBAC:

1. Role assignment: A subject can execute a transaction only if the subject has selected or been assigned a role.
2. Role authorization: A subject's active role must be authorized for the subject. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized.
3. Transaction authorization: A subject can execute a transaction only if the transaction is authorized

for the subject's active role. With rules 1 and 2, this rule ensures that users can execute only transactions for which they are authorized.

Additional constraints may be applied as well, and roles can be combined in a hierarchy where higher-level roles subsume permissions owned by sub-roles.

Most IT vendors offer RBAC in one or more products.

See Also

- Access badge
- Alarm management
- Biometrics
- Card reader
- Computer security
- Credential
- Door security
- Electronic lock
- IP Controller
- IP reader
- Key cards
- key management
- Lock smithing
- Lock picking
- Logical security
- Magnetic stripe card
- Optical turnstile
- Photo identification
- Physical key management
- Physical Security Professional
- Prison
- Proximity card
- Razor wire
- Safe
- Safe-cracking
- Security
- Security engineering
- Security lighting
- Security Management
- Security policy

- Smart card
- Swipe card
- Wiegand effect
- XACML

References

- en.wikipedia.org