ACCESS CONTROL

Access control is a system which enables an authority to control access to areas and resources in a given physical facility.

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.

PHYSICAL 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 guard with a device such as a turnstile. There may be fences to avoid circumventing this access control.

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.

Theory of 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.

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.

System Components

An access control point, which can be a door, turnstile, parking gate, elevator, or other physical barrier where granting access can be electrically 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 cases where exit is also controlled or anti pass back is required 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 (REX) is used. Request-to-exit devices can be a push button or a motion detector.

As a chain is only as strong as its weakest link, choosing the right locking device to block the door or the gate from opening is very essential for every access control system knowing that for every type of door there is a respective type of locking device such as electric strikes, magnetic locks, electric bolts, motorized locks...

Even though in almost all access control systems, the authorizations are given locally based on a local database, the setting/update of this database can be done centrally in online systems or locally with offline systems.

**Online Access Control System**

Online systems are very common in medium to large installations, especially where online monitoring is required. In these systems, Control Panels are connected to a host PC via a serial RS-232 communication line or Via TCP/IP. Readers, Electrical Strike (and/or Magnetic Lock) & Door Status Sensors are connected to Control Panel Control Panels are connected serially using RS-422 Communication Line (Max 32)

**Offline Access Control System**

Offline systems are very common in small installations with a minimal number of users, or in medium to large installations where online monitoring is not required, or in such a wide spread installation where it’s impractical to connect the various points together.

For that, the only way to update the authorization database is by carrying the authorization criteria with the media, meaning each credential would carry the information required to allow or deny the access, amongst the validity of the card, as well as its access level meaning the points it is allowed to open.

Usually such systems have a single or multiple encoding units to transfer the information into the credentials; this way, a
There are many card technologies including magnetic stripe, bar code, Wiegand, 125 kHz proximity, 26bit card-swipe, contact smart cards, RF and UHF contact less smart cards. Also available are key-fobs which are more compact than ID cards and attach to a key ring.

But credentials could also be biometric using various human parameters such as fingerprint, face geometry, hand geometry, iris and retina, and even voice, relieving those requesting access from carrying any cards, and eliminating the risk of card theft or borrowing.

**Barcode**

A barcode is a series of alternating dark and light stripes that are read by an optical scanner. The organization and width of the lines is determined by the bar code protocol selected. There are many different protocols but Code 39 is the most popular in the security industry. Sometimes the digits represented by the dark and light bars are also printed to allow people to read the number without an optical reader.

The advantage of using bar code technology is that it is cheap and easy to generate the credential, and it can easily be applied to cards or other items.

However the same affordability and simplicity makes the technology susceptible to fraud, because fake barcodes can also be created cheaply and easily, for example by photocopying real ones.

One attempt to reduce fraud is to print the bar code using carbon-based ink and then cover the bar code with a dark red overlay. The bar code can then be read with an optical reader tuned to the infrared spectrum, but cannot easily be copied by a copy machine. This does not address the ease with which

**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. 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.
bar code numbers can be generated from a computer using almost any printer.

**Magnetic Stripe**
Magnetic stripe technology, usually called mag-stripe, is so named because of the stripe of magnetic oxide tape that is laminated on a card. There are three tracks of data on the magnetic stripe. Typically the data on each of the tracks follows a specific encoding standard, but it is possible to encode any format on any track. A mag-stripe card is cheap compared to other card technologies and is easy to program. The magnetic stripe holds more data than a bar code can in the same space. While a mag-stripe is more difficult to generate than a bar code, the technology for reading and encoding data on a mag-stripe is widespread and easy to acquire. Magnetic stripe technology is also susceptible to misreads, card wear, and data corruption.

**Wiegand Card**
Wiegand card technology is a patented technology using embedded ferromagnetic wires strategically positioned to create a unique pattern that generates the identification number. Like magnetic stripe or bar code, this card must be swiped through a reader to be read.

Unlike those other technologies the identification media is embedded in the card and not susceptible to wear. This technology once gained popularity because of the difficulty in duplicating the technology creating a high perception of security.

This technology is being replaced by proximity cards because of the limited source of supply, the relatively better tamper resistance of proximity readers, and the convenience of the touch-less functionality in proximity readers.

**Proximity Card**
The Wiegand effect was used in early access cards. This method was abandoned in favor of other technologies. Card readers are still referred to as “Wiegand output readers” but no longer use the Wiegand effect. The new technologies retained the Wiegand upstream data so that the new readers were compatible with old systems. A Proximity reader radiates a 1" to 20" electrical field around itself. Cards use a simple LC circuit. When a card is presented to the reader, the reader’s electrical field excites a coil in the card. The coil charges a capacitor and in turn powers an integrated circuit. The integrated circuit outputs the card number to the coil which transmits it to the reader.

A common proximity format is 26 bit Wiegand. This format uses a facility code, sometimes also called a site code. The facility code is a unique number common to all of the cards in a particular set. The idea is that an organization will have its own facility code and a set of numbered cards incrementing from 1. Another organization has a different facility code and their card set also increments from 1. Thus different organizations can have card sets with the same card numbers but since the facility codes differ, the cards only work at one organization.

This idea worked fine for a while but there is no governing body controlling card numbers, and different manufacturers can supply cards with identical facility codes and identical card numbers to different organizations. Thus there is a problem of duplicate cards. To counteract this problem
some manufacturers have created formats beyond 26 bit Wiegand that they control and issue to organizations.

In the 26 bit Wiegand format, bit 1 is an even parity bit. Bits 2-9 are a facility code. Bits 10-25 are the card number. Bit 26 is an odd parity bit. Other formats have a similar structure of a leading facility code followed by the card number and including parity bits for error checking.

**Smart Card**
There are two types of smart cards: contact and contactless. Both have an embedded microprocessor and memory. The smart card differs from the card typically called a proximity card in that the microchip in the proximity card has only one function: to provide the reader with the card’s identification number. The processor on the smart card has an operating system and can handle multiple applications such as a cash card, a prepaid membership card, and even an access control card.

The difference between the two types of smart cards is found in the manner with which the microprocessor on the card communicates with the outside world. A contact smart card has eight contacts, which must physically touch contacts on the reader to convey information between them. Since contact cards must be inserted into readers carefully in the proper direction, the speed and convenience of such transaction is not acceptable for most access control applications.

RFID Card
The contactless alternative for the smart card commonly identified as RFID cards, uses radio transmission with higher frequencies compared to the proximity cards (UHF: 866 KHz & RF: 13.56 MHz instead of 125 kHz) hence allowing the transfer of more data between the reader and the card – in both directions – and simultaneous identification of several cards.

Most access control systems only read serial numbers of contactless smart cards and do not utilize the available memory. Card memory may be used for storing biometric data (i.e. fingerprint template) of a user. In such case a biometric reader first reads the template on the card and then compares it to the finger (hand, eye, etc.) presented by the user. This way biometric data of users does not have to be distributed and stored in the memory of controllers or readers, which simplifies the system and reduces memory requirements.

Smart cards have been targeted successfully by criminals in what is termed a supply chain attack, in which the readers are tampered with during manufacture or in the supply chain before delivery. The rogue devices capture customers’ card details before transmitting them to criminals.

Depending on the frequency used and the size of the antenna, and whether the card is passive or active (fitting with a battery) the reading range could vary between few centimeters to few meters.
Passive tags receive all of their power from the external tag reader, allowing the tag to “wake up” and transmit data. Tags also can be read-only (stored data can be read but not changed), read/write (stored data can be altered or rewritten), or a combination in which some data is permanently stored while other memory remains accessible for later encoding and updates. These tags could be produced as adhesive labels to be stuck on products (such as in libraries and retail stores) or on vehicles to distant identification (practical at toll roads or parking lots) with specific tags that are fixed on the number plates or windshield.

The most popular RFID cards on the market today using the 13.54 MHz frequency are:
- The Mifare cards, designed by Phillips, which are available in formats: the UL (Ultra Lite), the 1K, the 4K and the DesFire that have respectively more capacity to carry information on the holder or a copy of the transactions performed during all the readings, and different levels of security to access its content.
- The iClass cards, manufactured by HID, which are available in formats: simple RFID or in combination with other technologies

<table>
<thead>
<tr>
<th>Standards</th>
<th>U UHF (860-960KHz)</th>
<th>HF (860-960KHz)</th>
<th>HF (13.56MHz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols</td>
<td>EPC Gen2 (ISO 18000-6C)</td>
<td>ISO 15693</td>
<td>ISO 14443</td>
</tr>
<tr>
<td>Source</td>
<td>Developed by MIT Auto ID center and EPC global</td>
<td>Vicinity read, developed by ISO/IEC JTC1</td>
<td>Proximity read, developed by ISO/IEC JTC1</td>
</tr>
<tr>
<td>Read Range</td>
<td>3-5 meters+</td>
<td>1 meter</td>
<td>0.1 meter</td>
</tr>
<tr>
<td>Reader Cost</td>
<td>500-$3500</td>
<td>100-$1000</td>
<td></td>
</tr>
<tr>
<td>Tag Cost</td>
<td>$0.10-$0.20</td>
<td>$0.20-$0.50</td>
<td></td>
</tr>
<tr>
<td>Memory size</td>
<td>96 bits to 1 Kbits</td>
<td>256 bits to 8 Kbytes</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Read/write protection, anti-cloning, and no encryption</td>
<td>Multiple encryption/security features</td>
<td></td>
</tr>
</tbody>
</table>
such as magnetic, proximity, and offer a higher level of security than Mifare just because their production is restricted to one supplier.

As for the 866 KHz, the EPC global organization developed the UHF Gen 2 standard so users could accurately identify multiple items at distances not possible with HF RFID tags. The ISO ratified UHF Gen 2 as an international standard for use worldwide. Currently, UHF Gen 2 stands as the dominant RFID technology for supply chain applications, and is widely used for industrial automation, asset management, inventory monitoring, personal ID, and access control.

UHF Gen 2 RFID systems do not support encryption, and the data remains open and readable by anyone with equipment that complies with the protocol standard. Security provisions in UHF Gen 2 include multiple levels of write data protection, while some tags also offer read protection.

In addition, most UHF Gen 2 devices contain features to guard against tag cloning. Typically, cloning protection exists in the form of a Unique Identifier (UID) permanently encoded to the chip by the manufacturer. Several security features are optional, requiring activation during system setup. Users can encode additional data in the user memory, and apply separate levels of security to each memory block. By using the “permalock” feature, users can lock data into Gen 2 chip memory to prevent data rewrites.

By integrating wireless technology with the power of dynamic data storage, passive RFID technology extends the application space for asset tracking, supply chain management, and access control. The most effective RFID systems take advantage of IT integration technologies to support the organization’s unique value proposition and process requirements. With RFID, enterprises gain a flexible tagging solution that complements an existing bar code infrastructure and creates new opportunities for reducing costs and improving operational efficiencies.

**PIN**

A personal identification number (PIN) falls in the category of what you know rather than what you have. The PIN is usually a number consisting of four to eight digits – fewer and the number is too easy to guess, more and the number is too difficult to remember. The advantage to using a PIN as an access credential is that once the number is memorized, the credential cannot be lost or left somewhere.

The disadvantage is the difficulty some people have in remembering numbers that are not frequently used and the ease with which a PIN can be observed and therefore used by unauthorized people. The PIN is even less secure than a bar code or magnetic stripe card, but it is more versatile.

**BIOMETRICS**

There are several forms of biometric identification employed in access control: fingerprint, hand geometry,
Iris recognition, face recognition, voice recognition and recently introduced vein recognition. The use of biometric technology significantly increases the security level of systems because the templates relative to each individual cannot be duplicated – in the case of the finger, vein and iris – or are very hard to simulate – in the case of the voice, the face and the hand geometry. Moreover, biometric identification is practical as the users are not to remember a code or to carry a card that they could easily lose.

The operation of all biometric readers is alike: they compare the template stored in memory to the scan obtained during the process of enrollment. If the probability that the template in the memory and the live scan belong to the same person is higher than a preset threshold, the ID number of that person is sent to a control panel. The control panel, then, checks permissions of the user and makes the decision whether to grant access or not.

The communication between the reader and the control panel is usually done in the industry standard Wiegand protocol. Nonetheless, intelligent biometric readers exist with built-in time base and output relays that allow them to directly control door hardware. Biometric templates may be stored in the memory of readers, in which case the number of users is limited by reader memory size.

Readers currently available in the market may store up to 50,000 templates. Template of each user may also be stored in the memory of his/her smart card. This option removes all limits to the number of system users, but it requires each user to have a card and makes biometric-only identification impossible.

Biometric templates may also be stored in the memory of a central server PC. This option is called “server-based verification”. Readers simply read biometric data of users and forward it to the main computer for processing. Such systems support large number of users, but they are very much dependent on the reliability of the central server and communication lines.

There are 2 types of recognition:
- 1-to-1 mode: where a user must first identify himself/herself to the reader by either presenting an ID card or entering a PIN. The reader then looks up the template of the user in the database and compares it with the live scan. The 1-to-1 method is considered more secure and is generally faster as the reader needs to perform only one comparison. Most 1-to-1 biometric readers are “dual-technology” readers: they either have a built-in proximity, smart card or keypad reader, or they have an input for connecting an external card reader.

- 1-to-many mode: where a user presents his finger (or hand, eye, etc.) and reader needs to compare the live scan to all the templates stored in the memory. This method is preferred by most end-users, because it eliminates the need to carry ID cards or use PINs. On the other hand this method is slower, because the reader may have to perform thousands of comparison operations until it finds the match. An important technical
characteristic of 1-to-many readers is the number of comparisons that can be performed in one second, which is considered the maximum time that users can wait at a door without noticing a delay. Currently most 1-to-many readers are capable of performing 2000 - 3000 matching operations in one second.

Each of the biometric technologies on the market has certain advantages and disadvantages which must be considered in developing biometric systems, such as: system reliability, price, flexibility, necessity of physical contact with the scanning device and many others. Here is a brief on each of the most commonly used technologies.

**Fingerprint**

Fingerprint terminals can have 1 of 2 types of sensors: capacitive and optical.

The capacitive sensors correspond to the following needs:

- **Personal usage, without risk of vandalism**
- **Authentication 1:1 or identification 1:N for a small number of people**
- **Low number of captures per day**
- **Clean environment (office ...)**
- **Integration in slim line equipment**

The optic sensors correspond to the following needs:

- **Intensive usage, companies or industrial sites, for access control or time management**
- **Authentication 1:1 or identification 1:N on a few thousand people**
- **Difficult environment, sometimes polluted**
- **Risks of vandalism**
- **Could be coupled with electro-optic anti false finger device, the optic sensors only detect living fingers**
- **Because of the compact modules, the optic sensors can now be integrated into compact equipment**

In terms of cost:

- **The price differences between the optic sensors and the capacitive sensors are on a downward trend since the arrival of the compact optic sensors.**
- **Also, the robustness of the system should be taken into account; with a system that has already been installed, the replacement of a deteriorated capacitive sensor is far more expensive than to integrate from the beginning an optic sensor, and this is particularly true for the compact models.**

1 to 1 Fingerprint identification-matching speeds varies according to the size of the internal database – which can vary between few users to tens of thousands of users. Such identification in high-end physical access systems against a database of 1000 users can take 0.7 seconds while for 10,000 users could reach 1.8 seconds.

Typically, a rolled fingerprint has around 80 minutia points. These are the positions on a fingerprint where ridges split or end – as shown below. A damaged fingerprint could have >150 minutia points, of which some 50% may be false. If these false points are misinterpreted as true minutia, matching accuracy is severely compromised.

Consistently accurate fingerprint matching relies on algorithms that:

1. Detect and identify the positions of true minutia points
2. Predict the positions of obscured, distorted, or erased true minutia points
3. Recognize and exclude false minutia points created by injury, dirt, or liquid. The graphic illustrates a single ridge on a fingerprint. At each end of the ridge there is a termination marked by true minutia...
As hand geometry is not distinctive, it is the ideal choice. Furthermore, hand geometry data is easier to collect. With fingerprint collection good frictional skin is required by imaging systems, and with retina-based recognition systems, special lighting is necessary. Additionally, hand geometry can be easily combined with other biometrics, namely fingerprint. One can envision a system where fingerprints are used for (infrequent) identification and hand geometry is used for (frequent) verification.

Furthermore, these systems continuously learn all changes in the hand geometry, such if over time ones hand grows thinner, thicker, longer, ... The template of the hand will continuously be modified accordingly (taking an average between the past 3 accepted readings).

Face
Face recognition can be a practical alternative for selecting and developing an optimal biometric system. Its advantage is that it does not require physical contact with the reading terminal.

Hand Geometry:
Unlike fingerprints, the human hand isn’t unique. One can use finger length, thickness, and curvature for the purposes of verification but not for identification.

For some kinds of access control like immigration and border control, inversive biometrics (e.g. fingerprints) may not be desirable as they infringe on privacy.

In such situations it is desirable to have a biometric system that is sufficient for verification.

Infrared light launches the specific wavelength active light, shining the goal reflected off the target, the other impurities is filtered by customized filter, formed the high quality picture on the light-sensitive chip,
This multi-biometric approach also helps in situations where a certain biometric feature is not optimal for certain groups of users. For example, people who do heavy labor with their hands may have rough fingerprints, which can increase the false rejection rate if fingerprint identification was used alone.

* 10-20% of workers have problem with their fingerprint to get verified

**Iris Scanning**
Facial recognition technology has gained publicity post 9-11 for its ability to “scan” large crowds and populations (random travelers in airports, those attending public events such as the Super Bowl, etc.) As such, it can be useful as a non-invasive attempt to “pick out” those who might fit a similar description within a database, making it a good “surveillance” technology.

However, facial recognition is relatively easy to fool. Age, facial hair, surgery, head coverings, and masks all affect results. For this reason, it will most likely remain
a surveillance tool instead of a baseline identifier, and will not be used for critical: all match applications such as border control, Simplified Passenger Travel (SPT) or restricted access.

Some of the advantages of Iris Scanning are:
- Proven highest accuracy: iris recognition had no false matches in over two million cross-comparisons, according to Biometric Product Testing Final Report (19 March 2001, Center for Mathematics and Scientific Computing, National Physics Laboratory, U.K.)
- Efficiency: Ability to handle very large populations at high speed with low false rejection rates of 1: 1.2 million
- Convenient: all a person needs to do is look into a camera for a few seconds. A video image is taken which is noninvasive and inherently safe.
- Reliability: The iris itself is stable throughout a person’s life (approximately from the age of one); the physical characteristics of the iris don't change with age.

**LOCKING DEVICES**

As the final objective for an access control system is to allow or deny the access through a door, a gate, a barrier or a turnstile, it is mandatory to choose the appropriate locking devices to each of the above types of access point, that are directly related to their size and the material they are made of.

**Electric Strikes**

Electric strikes are the most common locking devices on the market. It replaces the fixed strike plate in front of a standard latch bolt. They come in 2 basic configurations:
- Fail-secure. Also called fail-locked or non-fail safe. In this configuration, applying electric current to the strike will cause it to open. In this configuration, the strike would remain locked in a power failure, but typically the knob can still be used to open the door from the inside for egress from the secure side. These units can be powered by AC which will cause the unit to “buzz”, or DC power which will offer silent operation, except for a “click” while the unit releases.

- Fail-safe. Also called fail-open. In this configuration, applying electric current to the strike will cause it to lock. In this configuration, it operates the same as a magnetic lock would. If there is a power failure, the door would open merely by being pushed/pulled open. Fail safe units are always run using DC power.

There are strikes for wooden doors, for metal doors, for narrow aluminum profile, or even glass doors. When choosing an electric strike one should also check its holding force which could vary between 500DaN (Kg) for standard wooden to 1000DaN for large metal doors.

One of the weaknesses of electric strike is their latch preload, which is the minimum force (around 10DaN) applied on the door that would block the strike from opening even when it is activated, and this weakness makes it unsuitable for emergency exits.

Last but not least, the choice of the lock case facing the strike is also important as it should offer a mechanical override (e.g. With secure cylinders), or better with guard bolts to prevent the latch from being pushed when the door is closed.

**Magnetic Locks**

A magnetic lock is a simple locking device that consists of an electromagnet and armature plate. By attaching the electromagnet to the door frame and the armature plate to
the door, a current passing through the electromagnet attracts the armature plate holding the door shut.

Unlike an electric strike a magnetic lock has no interconnecting parts and is therefore not suitable for high security applications because it is possible to bypass the lock by disrupting the power supply.

Nevertheless, the strength of today's magnetic locks compares well with that of conventional door. Power supplies incorporating a trickle-charged lead-acid battery pack can be used to retain security for short-term power outages, as this locking device is fail safe by definition, which automatically unlocks when the power supplying is cut.

Magnetic locks are suitable for double doors, are always powered with DC current, and could have holding forces from 100DaN to 1000DaN. They exist as shearlocks so as to be installed in the frames.

**Electric Bolts**

Electric bolts may be the most secure amongst all locking devices with holding forces reaching 600DaN.

They come in fail-safe or fail-secure, and can be concealed within the door frame which makes them more elegant than magnetic locks.

**Electric Lock Case**

Electric lock cases offer a high level of security especially when they feature the ADB (Automatic Dead Bolt) where not only the latch bolt is the part holding the door against the strike plate but also the dead bolt which goes easily 2cm inside the door frame, with no latch preload since the unlocking is done inside the lock case away from any external pressure.

Their main drawback is the fact that they are installed on the door and hence controlling them means having the control either on the door as well (such as in the case of the hotel electronic locks that are battery operated), or on the wall requiring a wire loop or electric hinge to feed the wires between the 2 parts.

Electric locks often come equipped with:
- A guard bolt to prevent pushing the latch bolt inside the lock when it is pushed inside itself against the door frame in the closed position.
- A friction free latch bolt to smooth the retraction of the latch bolt
- A monitored cylinder to be used as mechanical override but still monitored to indicate whenever it has been used
- A low power consumption solenoid based unlocking mechanism that is most convenient for battery operated locks ensuring more than 4000 opening with simple alkaline batteries.