INTRODUCTION

Access control is considered one of the three pillars of a comprehensive security solution, alongside video surveillance and alarm systems.

Access control essentially consists of two main components, the lock (i.e. the physical mechanism keeping the door locked) and the access control operation device (such as a card reader, biometric reader or keypad, which opens the lock).

Both of these components have a range of options available on the market, each suitable for different sites, scenarios and levels of security.

This white paper will help you gain an overall understanding of the key options available in access control, and ultimately help you better decide which solution best suits your needs.

IN THIS WHITE PAPER

<table>
<thead>
<tr>
<th>Part 1: Electric Locks</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electromagnetic Locks</td>
<td>4</td>
</tr>
<tr>
<td>Electric Strike Locks</td>
<td>5</td>
</tr>
<tr>
<td>Wireless Locks</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 2: Access Authorization</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘Something You Know’</td>
<td>8</td>
</tr>
<tr>
<td>‘Something You Have’</td>
<td>9</td>
</tr>
<tr>
<td>‘Something You Are’ — Biometrics</td>
<td>10</td>
</tr>
<tr>
<td>The Ideal High Security Authentication Solution</td>
<td>12</td>
</tr>
</tbody>
</table>

Conclusion 13
PART 1:
ELECTRIC LOCKS

In Part 1 of this white paper, we will take a look at the lock component, specifically electric locks. Electric locks are already widely adopted in the States and much of Europe, and their use is growing fast in Asia too as companies and individuals realize electric locks provide a safe and secure solution for access control.

This section covers the three main types of electric locks on the market. Taking into account the safety, security, convenience and aesthetics of each type, we'll provide you with an overview of the options available.

Quick Overview

Most electric locks can be set to function in one of the following ways:

- **Fail-safe**: in the event of a loss of power supply, the lock will automatically unlock, ensuring that people can still exit through the door (safety first)

- **Fail-secure**: in the event of a loss of power supply, the lock will automatically lock, meaning people are unable to enter (or exit) through the door (security first)

It therefore only takes a loss of power to make a fail-safe lock ineffective. Of course there can be a battery backup supply installed, but the battery will have a limited lifespan, perhaps not more than a couple of hours, which limits the time available for the power supply issue to be resolved. Fail-secure locks are therefore better for doors which require higher security, but carry greater risk for safety as there could be people trapped inside the building.
ELECTROMAGNETIC LOCKS

Accounting for about 80% of the electric locks in use, mag-locks operate by an electromagnetic strip attached to the door frame which aligns with an armature attached to the door. The lock can be fail-safe (whereby the electromagnet releases the armature) or fail-secure (whereby the electromagnet attracts the armature) depending on the use and safety standards.

Main advantages

Mag-locks are relatively simple to install and are cost effective in terms of procurement and installation. They are also fast to operate and can withstand significant mechanical force.

Main drawbacks

Fail-safe locks, which are most commonly adopted, require a constant supply of electricity to remain locked therefore making them slightly more expensive to run due to continuous electricity consumption. Moreover, if a mag-lock is continuously locked for a long time, it can be difficult to open. Another disadvantage is that the lock is essentially just a magnet so can be easily tampered with using everyday metal objects.
ELECTRIC STRIKE LOCKS

Electric strike locks account for around 10-15% of the electric locks in use. These locks are secured via a mechanical lock within the door and door frame which is connected to an electricity supply. The lock is therefore released if the access control device is activated (instead of using a key in traditional mechanical locks). Like mag-locks, electric strike locks can be set as fail-safe or fail-secure.

Main advantages

The major advantage of electric strike locks is that because the lock component works like a standard mechanical lock, the lock can be set such that it can be opened from inside using a handle. An electric strike lock can therefore be set as fail-secure, but still allow people inside the building to exit safely, without needing to install a break glass or release button inside. Locks can also be installed with a key lock option enabling the door to be unlocked mechanically too (particularly in case of a loss of power on a fail-secure lock).

Main drawbacks

Electric strike locks tend to be more expensive and more complicated to install as they require various components and wiring. Moreover, if the door can be opened with just the handle from the inside (rather than a release button) then it is impossible to track exits through the door on the access control system.
WIRELESS LOCKS

Wireless locks essentially work like a strike lock in terms of the mechanics, but the access control element is contained within the lock system on the door itself. It is therefore battery powered and the lock released via wireless technology.

Main advantages

Electric locks have fewer components so are cleaner looking and easier to install. This means that they can be easily added to a door at any stage on site construction (unlike wired doors which can be difficult to install after a site is complete). They do not require a break glass or push button device to override the lock like in mag-locks and electric strike locks. In addition, wireless locks only use electricity when the lock is being opened resulting in less energy consumption while safe and secure at all times. Although a wireless lock can be slightly more expensive option initially, they require less maintenance making them a cost effective option in the long run.

Main drawbacks

As a battery powered device, users should be alert and responsive to when the lock’s battery is running low, as if not replaced, the lock will not be able to be opened electronically.
PART 2:
ACCESS AUTHORIZATION

Each of the lock components described in Part 1 need to be configured with a ‘systems operation device’, a mechanism which authorizes access and allows the lock on the door to be opened.

In Part 2 of this white paper, we will therefore provide an overview of the types of access control operation devices on the market and the points of consideration around them. Due to the recent and ongoing debate about using biometrics as a form of authorization, this section will include a particular focus on this form of technology.

In access control, there are three fundamental methods for verifying authorized access:

- Something you know: such as a password, a PIN, or a code
- Something you have: such as a key, an access card (or badge) or a mobile device
- Something you are: a physical trait, such as a fingerprint, also known as biometrics.
‘SOMETHING YOU KNOW’

Authentication as ‘something you know’ is typically a password, PIN or code which, if entered correctly, will grant the user access. Often used in access control, this method of verification is also commonly adopted in banking and to verify access to accounts such as email or other online accounts.

Such verification is both easy and convenient to use although can pose issues or inconvenience if a password or PIN is forgotten.

The primary risk of breach of security with this method of authorization comes from a violated password. Passwords and PINs may be hacked or cracked, be shared (intentionally or not) or be leaked, any of which would give access to unauthorized personnel. To help avoid (but not eliminate) this problem, ideally passwords should be changed regularly. However, this can make remembering the correct password more of challenging.

This type of authentication is more often seen in access control solutions for private properties or smaller companies rather than in companies or organizations with a large number of employees and a large number of access control points. The reason for this is that this option can becomes increasingly complicated and impractical and even less secure if multiple passwords are used or the same password is used for multiple doors or personnel. There are therefore limitation in the scalability of the solution.
‘SOMETHING YOU HAVE’

Authentication which is ‘something you have’ is most often an access card (or badge) or a key. Keys are typically used for access control in private residences and rarely used for doors at large sites. This is due to the additional capabilities and the practicalities of using key cards, as described below.

Key cards are ideal for most corporate site solutions as they are scalable and easy to manage via an access control management platform in which employees can be added and removed. Moreover, the solution is flexible as access limited to certain levels or times for different employees.

Although this access via card readers presents a risk if the card lost or stolen, this risk may be significantly reduced or eliminated if reported immediately. If reported, access with that card can be removed through the management platform, essentially rendering the card useless.

Key card technology is difficult to forge as the technology used is sophisticated, including microchips and radio technology which are embedded within the card itself.

Another more recent addition to this type of access authorization is using a mobile phone to gain access like a key card. Mobile contactless credentials act as ‘virtual keys’ which can be stored in a mobile handset and used to unlock doors by swiping the mobile like a key card. One of the major advantages of this option is that access can be instantly delivered to a person’s handset remotely; no physical handover is required.
‘SOMETHING YOU ARE’ - BIOMETRICS

In comparison to other forms of access authorization, the use of biometrics in access control is a more recent phenomenon.

Biometrics describes a physical feature unique to a person which can therefore be used to identify that person. Types of biometric authentication include fingerprints, irises, facial recognition through contours and features, hand geometries, vein patterns, voice patterns and DNA information.

In addition to being adopted for access control, recent years have seen a surge in debate about using biometrics for other forms of identification and authorization. For example Apple incorporated a fingerprint reader feature in their new iPhone 6 which can be used to authorize payments from your bank account via your mobile. It was also announced last week that MasterCard has partnered with Norwegian company Zwipe and are working towards being able to offer credit card payments via fingerprint scanning by November 2015. Another more extreme example is of a New York based company that wants to introduce biometrics which will be able to grant access to a building through analyzing the way a resident walks.
The Risks

Biometrics appear to be an ideal solution for authorization verification as the physical traits used are unique to each person. However, biometrics are not exempt from risk.

Somebody's physical identity can too be compromised (basic kits to replicate and fake fingerprints can be bought online), and once such information has been compromised, it will always be compromised. Unlike a password or PIN, one's biometric identity cannot be changed.

As early as 2006, Deloitte and Touche were ringing the alarm bells warning that faking biometrics was a real threat. In fact, soon after the release of Apple's iPhone 6, reports were published that the phone's biometric identification can be faked. It's not easy, but it is possible.

Risk associated with different forms of biometrics varies, some forms of biometric authorization are more secure than others:

<table>
<thead>
<tr>
<th>Type of biometrics</th>
<th>Security</th>
<th>Cost</th>
<th>Size of device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint recognition</td>
<td>Medium</td>
<td>Low</td>
<td>Small</td>
</tr>
<tr>
<td>Finger vein patterns</td>
<td>High</td>
<td>Medium</td>
<td>Small to medium</td>
</tr>
<tr>
<td>Palm vein patterns</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Facial recognition</td>
<td>Low</td>
<td>Medium</td>
<td>Medium to large</td>
</tr>
<tr>
<td>Iris recognition</td>
<td>High</td>
<td>Medium to high</td>
<td>Large</td>
</tr>
</tbody>
</table>

The Reality

A recent survey of security integrator companies by IPVM, an impartial third party in the security industry, found that the demand for biometric solutions in security is actually still quite low. The most popular type of biometrics opted for from the above was fingerprint recognition at 49%, but 44% of integrators chose to use no biometrics at all.

The possible reason for this apparent reluctance to implement biometrics in access control is because many professionals think that the technology is largely under-developed and needs further technological progress. Moreover, some companies hold back from adopting biometrics for fear of conflicting with local privacy restrictions or of infringing on the personal privacy of employees or personnel.
THE IDEAL HIGH SECURITY AUTHENTICATION SOLUTION

A common solution when there is a strong need for high levels of security is to use multiple types of authentication methods.

For example, at ICD we recommend that some companies or sites use a combination of key card access with a PIN code where an extra layer of security is required. This solution is convenient as it can be tailored to end user’s needs by adjusting the settings in the management platform. For example, if such a device is installed at the main entrance of an office, the authentication can be set to card only during the day when the office has is busy with employees and there is constantly someone at the reception desk. With key card access only during these hours it is not only more convenient for employees, but in addition, the risk is not increased since an intruder will be noticed by any on-site staff. For after office hours or on weekends or holidays, the device can be set to require both a key card and a pin code to provide the extra layer of security necessary when no company personnel are on-site. Anyone who may have found or stolen the key card will therefore not be able to enter the site with the card alone.

An area of a site could also be equipped with a combination of key card and biometrics for higher security. This solution is common in areas where an extremely high level of security is required such as bank vaults, nuclear power plants and data centers.
CONCLUSION

Before you make any decisions about what access control solutions are best for your site, it’s important to first think carefully about what your site requires in terms of safety, security and convenience, and to fully evaluate how risk can be reduced to ensure that security related incidents won’t interrupt your business operations. Understanding these basic requirements will help significantly in the process of deciding which lock and access authorization type should be implemented.

It may also be relevant to consider the state of your site as if your access control just needs to be upgraded, a solution like a wireless lock is much easier to install than either an electric strike lock or a magnetic lock due to the lack of wiring.

End users often choose to implement several different types of access control solutions (both locks and authorization) in one site across different areas of the site and where different levels of security are required. It is therefore important to evaluate the level of security each area needs as well as considering the type of authorization and lock component that is best suited for that specific site and scenario.

To find out more about options in access control technology, please feel free to get in touch with our security experts at any of our regional offices via sales@icdsecurity.com.