What Type of Access Control Reader Should I be Using?

Over the years much has been written about the different types of access control readers: proximity card readers, multiclass card readers, card readers plus keypad, all types of biometrics readers. Some articles espouse the virtues of different types while others note the downsides. However, what end users ultimately want to know is 'what's best for me and why?'. While the answer to that question can in many cases be subjective and not easy to come by, there are certain criteria that can be used to help in the decision-making process.

There are three descriptions for the generally accepted levels of access control security: 'what you have', 'what you know', and 'who you are'. The use of any one of these levels by itself is called a single authentication use. The security industry has the fancy name of multifactor authentication to describe when multiple of these levels are used at the same time, but the bottom line is that all types of readers fall into one or more of those security levels. To determine what type of reader is appropriate for each application, first it must be determined what access security level or combination of levels makes sense.

The clear majority of applications, probably well over 90%, require only the 'what you have' access security level. This category includes proximity card readers and multiclass card readers with the use of an access card or keyfob. Card readers are almost always part of an overall electronic access control system where centralized access privileges and auditing are desired. These types of readers are very reliable, relatively easy to administer, and easy to use. Not surprisingly, they are also the least expensive type of reader. These readers offer a reasonable level of security for most entry points including exterior entrances and interior areas where there is a desired restriction of access. If the access control system is used in conjunction with a camera system or burglar alarm system that level of access security becomes even more sufficient.

Smart cards, used with multiclass readers, have a chip installed within the card that make the card less susceptible to duplication and are more durable. While smart cards may be part of a dual authentication process for financial transactions or laptop access in conjunction with a passcode, for security card reader purposes, the only security level is still possession of the card, 'what you have'. It's a great product and is widely used, but for most security system uses it's a single authentication product.

While for most access control deployments such a card reader provides a reasonable and acceptable security level, it should be noted that this is the case only with proper operational protocols in place. These include procedures to report and un-program lost or stolen cards, teach and enforce an anti-tailgating policy, and teach and enforce to never give your card to anyone else. Without these protocols in place, even an access point deemed acceptable for a single authentication reader will fall short of expectations and not provide reasonable security at those entry points.

The next level of access control security is 'what you know' and in an electronic access control system is almost always used in conjunction with 'what you have' to form a dual authentication process. The most common of these devices is the card reader plus keypad all in one unit. They are slightly more expensive than card only readers and the throughput rate, meaning how many people can use the reader and move through the access point in a given time, is not greatly affected. Some potential applications for this dual authentication include an executive's office door, a sensitive data closet, or file room subject to privacy laws. Basically, an application where the possibility of an unauthorized person possessing and using an authorized access card just doesn't provider an acceptable level of security.

Just as with the card only readers, this extra layer of authentication is only effective if accompanied with proper policies to define its use. For instance, not only should one never give someone else the access code but that code should not be on a sticky note somewhere for everyone to see like so many burglar alarm and computer access codes so recklessly displayed. There are uses for the 'what you know' keypad by itself even when it is not part of an overall access control system. This would now be considered a single rather than dual authentication reader, but when no auditing is required and there are very few readers to program, this may be an effective solution.

The third and arguably most secure level of access control security is 'who you are' and is most commonly associated with biometric readers such as fingerprint identification, retina or other type of eye scanners, facial recognition systems, and hand geometry readers. While sometimes biometric readers are used as a stand-alone device for access, the clear majority of the time they are used in conjunction with a 'what you have' card reader or 'what you know' keypad. This is accomplished as either two stand-alone devices that must both be activated in conjunction with each other or as a combined manufactured unit. It is extremely rare for all three levels of access security to be used at one access point for triple authentication, but it can be done.

So, where would one want such a reader? For areas requiring that extra layer of security or compliance. Data centers, financial institutions, and medical facilities are probably the most common private sector application; they are used in sensitive government facilities most often, including correctional facilities and in the military.

Unfortunately, there are tremendous downsides to the use of biometric readers, such as they are inherently unreliable. At best, fingerprint readers and eye scanners have a 98% success rate. That means at least two out of every hundred times the reader is used, it will deny access to an authorized user or allow access to an unauthorized one. That creates an administrative nightmare and the requirement of stringent and fast acting response policies to deal with those issues.

While facial recognition and hand geometry readers are more reliable, user enrollment and system administration are difficult. With all the biometric readers, the throughput rate is significantly diminished, meaning these readers only make sense on low traffic access points

because of the increased time per person it takes to use the reader and unlock the door. Again, not surprisingly, biometric readers are the most expensive type, sometimes many times more expensive than card only readers. All this is not to say that there aren't any appropriate applications for the 'who you are' biometric readers, there certainly are. It's just important to know what the pros and cons are before choosing this option.

Ultimately each end user needs to decide what level of access security they feel is required at each of the access points they want to protect. Factors may include what is in the area of controlled access, how those readers are used in conjunction with an overall access control system or other security systems in the facility, what are the cost implications, and what will be the traffic through that access point. Those answers will drive what type of access reader is appropriate for each application. Consulting a security professional to help guide the end user through that decision-making process should be considered.