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

Card Reader.

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

1. General

A card reader is anything, usually an electronic device that reads 'cards'. There is a wide variety of things called cards and hence there are many things called 'card readers'. For instance, paper punched card readers were used throughout the first several decades of the computer industry to store information and write programs for computer systems.

This article refers to modern, electronic devices that read or communicate with plastic cards with barcodes, magnetic strips, computer chips or other facilities on the card.

A memory card reader is a device used for communication with a smart card or a flash memory card. A business card reader is a scanning device used to scan and electronically save printed business cards. A magnetic card reader is a device used to scan cards containing magnetic data strips, such as credit cards.

2. Smart Card Readers

A smart card reader is an electronic device that reads smart cards. Some keyboards have a built-in card reader. There are external devices and internal drive bay card reader devices for PC. Some laptops have built-in smart card reader.

Some have a flash upgradeable firmware. The card reader supplies the integrated circuit on the smart card with electricity. Communication is done via protocols and you can read and write to a fixed address on the card.

3. Access control card reader

Access control card readers are used in physical security systems to read a credential that allows access through access control points, typically a locked door. An access control reader can be a magnetic stripe reader, a bar code reader, a proximity reader, a smart card reader, or a biometric reader.

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

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

b. Biometric

There are several forms of biometric identification employed in access control: fingerprint, hand geometry, iris and face recognition. The use of biometric technology significantly increases security level of systems because it eliminates such problems as lost, stolen or loaned ID cards, and forgotten or guessed PINs. The operation of all biometric readers is alike: they compare the template stored in memory to the scan obtained during the process of identification. If the probability that the template in the memory and the live scan belong to the same person is high enough, 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. The only exception is intelligent biometric readers that do not require any panels and directly control all 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 finger-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.

1-to-1 and 1-to-many are the two possible modes of operation of a biometric reader.

- In the 1-to-1 mode 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.
- In the 1-to-many mode 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.

c. 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.

d. 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.

e. 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 their 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.

f. 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 pre-paid 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 and the orientation has be observed the speed and convenience of such transaction is not acceptable for most access control applications. The use of contact smart cards is physical access control is limited mostly to parking applications when payment data is stored in card memory and when the speed of transactions is not important. A contactless smart card uses the same radio-based technology as the proximity card with the exception of the frequency band used: higher frequency (13.56Mhz instead of 125 kHz) allows to transferring more data and communicating with several cards at the same time. A

contactless card does not have to touch the reader or even be taken out from a wallet or purse. 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.

Smartcard readers 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.

g. 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.

4. References

- en.wikipedia.org