

Are You Protected by a Piece of Plastic and Two Screws?

Wiegand Had Its Day! Borer All-in-One Solution, will Ensure Your Data is Secure

Borer White Paper – October 2007

Introduction to Wiegand

The majority of cards and biometric readers in access control systems use a Wiegand interface to transmit data read from a card to a control panel. The control panel will then validate the data received and grant/deny access.

Often people in the Access Control Industry accept the Wiegand interface as a standard. Wiegand is not a standard as there is no formal definition, ratified by ISO or the IEEE, of the Wiegand Interface against which manufacturers can measure the performance of their equipment.

Wiegand is more of an informal working convention, which has allowed the manufacturers of card and biometric readers using a variety of reading technologies to connect their products to control panels produced by system integrators.

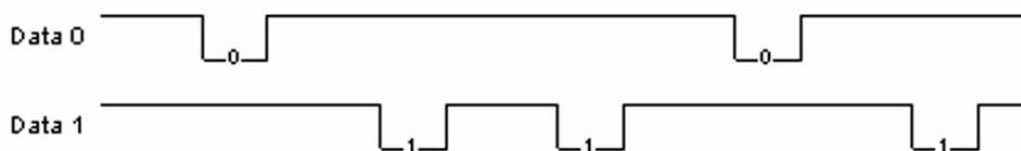
Originally Wiegand referred to a card reader technology consisting of a plastic card with two rows of metallic wire bars, which when a bar passed in front of a magnetic field and sensor circuit, generated a small electronic current.

The means by which this signal was passed to a control panel, the Wiegand interface, has since become a convenient convention for the transmission for data for the majority of card and biometric readers.

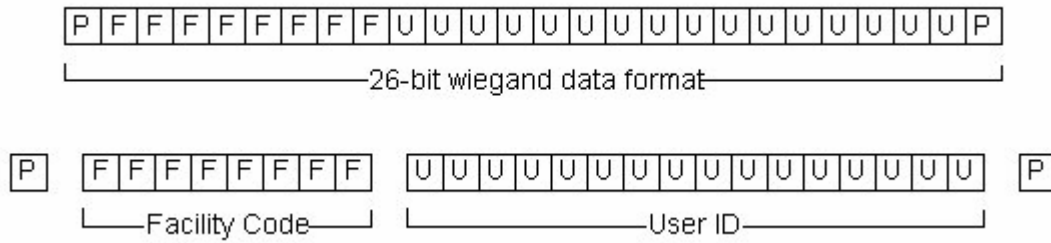
Wiegand Explained

Wiegand is a three wire electrical interface first employed in the 1970's and still being used today by a majority of card reader manufacturers, which is designed to enable a card reader made by one manufacturer to pass data, read from a card to a control panel produced by a different manufacturer.

It consists of three wires called "Data-0", "Data-1" and "Ground". A short pulse on the "Data-0" represents a binary "0" while a pulse of the "Data-1" represents a binary "1". The picture below is a graphical representation of a Wiegand data stream for the binary value "01101". Each dip in the line represents a change from 5V to 0V, thus communicating the bit value.

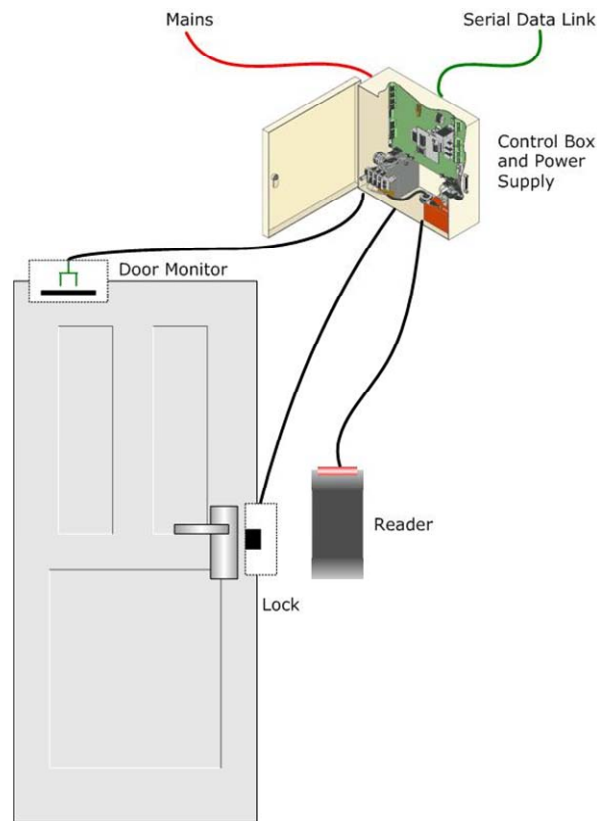


Wiegand data format is represented by the total bit count and the distribution of data fields on a card. The figure below illustrates the use of 26-bit Wiegand, the most commonly used Wiegand data format.



This Wiegand format consists of a parity bit, 8-bit facility code, 16-bit user ID, and parity bit, for a total of 26 (1+8+16+1=26) bits.

With this basic understanding of how to translate the information in the 26-bit Wiegand format, you can apply a similar convention to decode the data in any other data format passed over a Wiegand interface. Once you know the distribution of the data fields, you can extract the facility code and user ID fields.



Typical Solution using a Wiegand Reader
Physical connection between reader head and controller. Vulnerable to attack.

Wiegand has been Compromised

At the Defcon security conference on August 2007, a hacker and Defcon staffer who goes by the name Zac Franken, showed how a small homemade device he calls "Gecko", which can perform a hack on the type of access card readers used on office doors throughout the country.

"Gecko" is simply a small, programmable PIC chip with a wire connector on either side. Once it's connected to the wires behind the card reader, it's not only trivial to use a 'Replay' card to get through the door, but you can also disable the system so that nobody else can come in behind you.

What's more, making a "Gecko" is easy and cheap. Franken says the hardware costs about \$10 (£5).

According to Franken, the hack subverts the Wiegand protocol, commonly used for communication between the card reader and the back-end access control system, and doesn't take direct advantage of any problems with any of the hardware involved. When you swipe your card at the office door, the reader sends a signal using the Wiegand protocol to the control panel, which once the card has been validated, opens the doors.

Franken's demonstration showed how to hack into a card access reader by:

- Popping the card access reader's plastic cover (most card readers used in access control applications do not have tamper protection);
- Undoing two retention screws and exposing the electrical cable which connects the card reader to the control panel;
- Introducing a miniature circuit board onto the Wiegand data transmission lines and replacing the card reader head.

Following the introduction of the hacking device, each time a card is read its data can be recorded, as well as recorded and replayed at will. A hacker, looking to gain unauthorized entry, could simply record for replay at a later time a valid access transaction, without having any prior knowledge of the access credentials (identity card or biometric template).

Consequently, the majority of access control systems are vulnerable at their weakest point, the "**Wiegand Interface**" no matter how sophisticated the levels of security employed in protecting the identity card and the data held within it.

Extracts from the demonstration are available on Youtube:

http://www.youtube.com/watch?v=MHNJoHc_XDY

Protecting your Secure Identity Card

Users appear to be unaware that the security afforded by modern contact-less smart cards, can be easily compromised by the Wiegand Interface, which is still used by the majority of card readers.

Even very secure card technologies such as Mifare and Legic are vulnerable when data read from the card is sent as plain text across an insecure electrical connection.

Most modern card access readers, employ smart card technologies such as Mifare, which consist of an antenna and small circuit board with a Wiegand interface. This is connected via a signal cable to a separate controller.

The encrypted Mifare card data is detected by the antenna and the information read from it and decrypted into legible data by the reader, after which it is sent to the door access controller over signal cable using the security industry standard "Wiegand" interface and often a published open format "Wiegand" protocol.

The logic in providing a very secure interface between the card and reader head while maintaining an insecure connection between reader head and controller is questionable, since it is relatively easy, on the unprotected electrical interface to intercept the unprotected Wiegand data stream and/or inject false data into the data stream. Indeed most Wiegand style card readers even lack a simple tamper sensor so that any attempt to compromise or remove the reader head will go undetected.

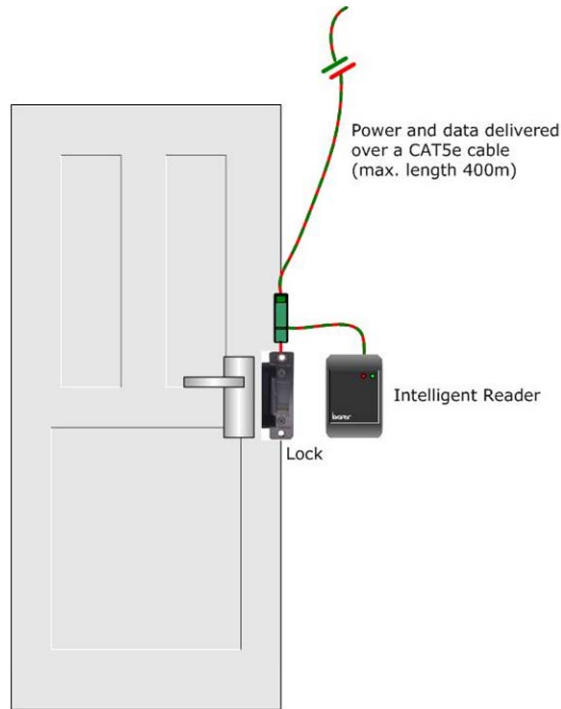
This compromises the high level of security built around the smart card and card reading technology. Hence, it is evident that data read from a secure and encrypted smart card, such as a Mifare or Desfire, when passed across an unprotected Wiegand, Magnetic Stripe or RS232 interface is open to skimming and manipulation.

In the past, proximity readers have been simple devices with no special configuration requirements. The introduction of smart card technology into access control has added an additional level of complexity and a further potential opportunity to compromise security. Before a smart card reader can be used, it must be configured with specific information such as the address of the card sector to be read from the card together with its' associated encryption keys.

Most Card Reader heads use a Wiegand or clock and data interface, which is a unidirectional communications path in that it only allows the data to be transmitted from card reader head to control panel. Consequently, all configuration change must be introduced on site at the card reader head. Such changes are often done by power resetting the reader before presenting a configuration card to the reader.

This introduces a further security risk in that the user or installer has to carry around configuration cards which are susceptible to being misplaced, lost or stolen. This procedure is also time-consuming and inconvenient because all changes must be performed by visiting every location.

This increases the time taken to introduce any alterations, such as a change of encryption key, especially over geographically diverse locations.



Borer Solution

Logical connection. Resistant to attack as data is encoded and can be encrypted.

Borer will Ensure your Data is Secure from Card to Database Server

Borer has worked to eliminate security deficiencies by combining the functions of antenna, card reader decoder and controller into a “single integrated intelligent card reader”. All information is exchanged at the logical network level where the data is encoded and when required encrypted.

This eliminates the transmission of secure data across an insecure electrical interface. Consequently, data from the card to the central database is secure and safe from being compromised.

A further benefit of the Borer integrated card reader and controller is that it allows the user to configure the reader over the network. Hence, changes can be simply, securely and quickly introduced.

The Borer intelligent card reader is installed on the unsecured side of the door. For added security, to prevent the door unlock signal being tampered with, the Borer reader is logically associated with a separate Lock Manager. This is located on the secure side and controls the operation of the door.

You can employ a second Borer Intelligent Reader to provide in and out control, or you can use a dedicated Lock Manager to monitor and control the door lock. Communications between the Borer intelligent card on the unsecured side of the door and the lock controller on the secured side is across the Controller Area Network (CAN) data link.

This solution maintains both signal and data integrity and provides a secure solution which is very difficult to hack into.

Related Articles:

- **2 Screws, 1 Plastic Cover, How Many Airports Infiltrated?**
(<http://www.eweek.com/article2/0,1759,2167540,00.asp>)
- **Simple Hack Can Unlock Most Any Office Door**
(<http://blogs.pcworld.com/staffblog/archives/005079.html>)
- **Open Sesame: Access Control Hack Unlocks Doors**
(<http://blog.wired.com/27bstroke6/2007/08/open-sesame-acc.html>)

Tel: +44 (0)118 979 1137 UK Tel: (0)845 155 9623 Fax: +44 (0) 118 977 3526 Email: info@borer.co.uk

Borer Data Systems Ltd, Crown House, Toutley Road, Wokingham, Berkshire, RG41 1QN

Web: <http://www.borer.co.uk> Registered in England No. 1207085