APPLIED WIRELESS ID

Applied Wireless Identifications Group, Inc.
18300 Sutter Boulevard, Morgan Hill CA 95037 • Voice 408-825-1100 • Fax 408-782-7402

Technical Reference

PROXIMITY CREDENTIALS – A SECURE TECHNOLOGY

Change History

Version	Date	Author	Comments
1.0	19 Mar 2008	LH	V1

For more than four decades, the proximity technology used in hand-held cards and other tokens has served the access-control security market safely and reliably. These notes show why proximity has become the favorite encoded credentials for access control and other secure applications.

History

The "proximity" technology has been used in encoded devices for identification and access control since the 1960s. Early proximity devices were limited to academic study because of the practical limitations of credential* size, number of available codes, and cost. The integrated circuit made it possible to embed an assembly of IC, printed-wiring board, and radio antenna in a card that could be handled easily and safely. This led to the first commercial applications in the 1960s. Cardkey was an early integrator of proximity cards into access control systems.

Rapid growth in other encoded card technologies kept proximity in the background for the next two decades. Magnetic stripe, barium ferrite, bar code and Wiegand effect offered flexibility in credential style, large code capacity, and reasonable cost for a growing market. (The popular photo ID badge may be combined with any of these digital encoding technologies.)

In the 1980s proximity entered its long and eventually successful market development program, based initially on supported prices that made the product increasingly competitive and in demand. In the 1990s proximity became a major player in the field of encoded credentials for identification of cardholders*, primarily for control of physical access through locked doors and gates. In the 2000s proximity credentials share the market with magnetic stripe cards. Proximity is dominant in security applications, while low-cost magnetic stripe remains popular in financial applications (credit and debit cards, ATM cards, purchase tokens, etc.). Barium ferrite, Wiegand effect, and infrared-transmission bar code have largely disappeared from the scene.

Technology

An important appeal of proximity during the early development years was its use of "radio" – two-way communication of digital code. Other credential encoding technologies seemed archaic when compared with this electronic digital encoding method. Proximity satisfied the public fascination with new science. Access system developers kept the interest alive by offering proximity as an available option, even when the other technologies were almost always selected by the end users.

Proximity's use of radio transmission required regulation by the U.S. Federal Communications Commission. After some early experimentation with transmission frequencies, the FCC assigned a band around 125 kilohertz (not far below the band used by AM commercial radio (540 kHz to 1600 kHz). The FCC set limits on bandwidth and effective radiated power for the devices.

The more recent "smart card" is similar to proximity in its use of two-way radio transmission between the credential and the reader. The major differences are expanded memory in the smart card's integrated circuit, and read-write capability. Many of the devices that read the card's code must also contain code-writing capability for renewal of stored cash value, for updating the card's database, etc.

Description of Proximity Technology

The proximity products in all installations are a combination of two transceivers – a reader that is usually mounted on a wall near the controlled door, and a credential that is usually held by the cardholder.

The proximity reader contains electronic circuits and a radio antenna, in a plastic housing. There are two independent circuits – a transmitter and a receiver. The reader's single antenna is shared by the transmitter and the receiver. The transmitter generates a radio-frequency field in all directions around the housing.

The proximity credential is essentially a miniature of the reader in concept. It is termed "passive"*; that is, the credential receives its electrical energy from the RF field that is generated by the proximity reader. When the credential is held in the effective radio field generated by the reader, the credential's electronic circuits are energized. They are then able to receive digital data from the reader, and to transmit the credential's own digital data to the reader. When the credential is removed from the reader's effective field, the credential becomes electrically dormant, incapable of any activity.

Security

This is the point at which security becomes an issue. The proximity reader is not only generating an RF field; it is also transmitting a particular code – a sequence of binary data that serve as a "hand-shaking" signal for the credential when it enters the reader's field. The credential must operate in the reader's bandwidth. It must recognize the unique binary code that the reader transmits to it. And it must be able to respond to the reader.

If the credential recognizes the reader's hand-shaking signal, the credential reflects a part of the reader's transmitted code back to the reader in the credential's own transmission. The credential also inserts the special identity code that AWID programmed into that credential when the credential was prepared for the customer's order.

The reader then uses its receiver mode to analyze the code that the credential transmitted to the reader. If the reflected code is correct for that reader, and if the credential's special identity code is in the proper format, and if the credential's repeated code transmission is identical for several consecutive events, *then* the reader accepts that credential as a valid AWID credential. The reader strips out the credential's special identity code and transmits just that code electrically on the reader's outputs.

Most AWID readers are supplied with two interface circuits that transmit the credential's identity code almost simultaneously. These are the Wiegand protocol electrical interface, and the ANSI RS-232 standard serial interface.

We have described the AWID proximity procedure. This description applies in general to all commercial proximity readers and credentials. Each commercial manufacturer of readers and credentials uses its own characteristic hand-shaking signal. Therefore credentials from a different manufacturer will not recognize a different hand-shaking signal from the reader. In that case, the credential will not transmit its own code back to the reader. The reader remains quiet and sends no identity code through its interfaces to the host system.

Code Formats

Another aspect of the security of the proximity technology is the availability of a variety of code formats. In its simplest form, the format is based upon the total number of binary bits, the number of data fields, the number of bits in each data field, and error-checking bits. The popular Wiegand-type international standard code is a format with 26 bits total, 2 data fields, and 2 error-checking bits. This results in more than 16 million distinct binary codes. The credentials for a particular site are commonly assigned 1 of 255 available site codes (or facility codes). Each individual credential at that site has 1 of 65,535 available ID numbers (or card numbers, or PINs).

Other formats may have a larger number of available codes – more data fields, more site codes, more ID numbers. They all offer the same degree of security through their technology, which is the same for every proximity token.

What Can an "Outsider" Do

There is an accumulation of factors that produce the basic security of the proximity technology:

- Low power – The effective radiated power of the proximity reader is very low. The effective radiated power of the credential is much lower. Unauthorized detection of code in the RF transmission is difficult to achieve.
- Encoding – All communications between reader and credential, and between reader and host system, are in code. Probability of understandable data that are available to an intruder is very small.
- Wiegand interface – The electrical transmission of the credential's code is most commonly on the Wiegand interface. It uses separate data lines for binary-0 and binary-1 bits. Every time slot in the serial transmission contains either a 0 bit or a 1 bit. These bits look identical electrically, except that they are on separate parallel wires. Outside observation would show just a string of pulses, not identifiable as 0 or 1.
- Password control of access to encoders – Programming of codes into new, unprogrammed credentials must be done on a special instrument that was developed by AWID for its own use. The programming is regulated by AWID's PC, which uses password protection.
- Password control of access to the application program – Access to the customer's system is always limited to an authorized operator, who uses a password to enter the programming phase of system operation.
- Control of access to AWID's products – AWID does not sell its products to end users, nor to any customer that is not known to the AWID's personnel. Customers are authorized only after considerable investigation.

How can an "outsider" compromise a system with AWID's proximity readers and credentials? Let's assume that an unauthorized person *were* able to read and interpret the code in a credential. To what use could the outsider put the data? That person would need access to AWID's code programmer to produce a spurious credential. That person would need the password. That person would need the special knowledge to set up a new credential.

Or, if the outsider had access to the wiring of the user's system, that person might somehow transmit a series of bits to the system. The person would have to know the significance of the wiring, and the exact nature of the data pulses (timing, amplitude, polarity).

The success of unauthorized activity in a proximity system is technically possible, but extremely unlikely.

Conclusion

One of this writer's first lessons upon joining the access-control security industry was this.

1. The major contributor to the security of an access control system is the *perception* of incorruptibility of the system. The fact that the user has invested the time and effort and cost of installing an access control system is vital to the effect that the system has on the facility's security.
2. Strong mechanical components are a vital component of the reliable system. The system is no more secure than the determination of the outsider to break the door. This is the legendary "size of the hammer" syndrome . . . If a little hammer won't break down the door, get a bigger hammer. The door and lock must prevent this.
3. The accumulation of special knowledge and special equipment in the system effectively excludes the unauthorized person from compromising the safety of the system.

* Glossary

Cardholder........The person who possesses the credential.
Credential.........A token that carries identification data for the person or vehicle to which it is assigned.
Passive.............Containing no internal battery for power; obtaining its power from an external energy field.