Smart Cards: Dumb & Dangerous Ways to Use Them

Contactless smart cards are fast becoming the technology of choice for access control applications. Security, convenience and interoperability are the three major reasons for this growth. However, in the move toward interoperability, reader manufacturers are offering readers that bypass all of the cards security mechanisms and instead read only the Smart Card? Serial Number (CSN). Reading only the CSN on a contactless smart card for access control security actually provides a false sense of security analogous to installing a high security door without any locking mechanism.

Understanding this misuse of the CSN is critical for users of the technology to ensure that access control security is maximized. If implemented and deployed properly, contactless smart cards represent one of the most secure identification technologies available today.

By Michael L. Davis

Michael L. Davis is the Director of Technology in HIDs Intellectual Property Department (**www.hidcorp.com**).

Why Use Contactless Smart Cards?

Contactless smart cards incorporate advanced state-of-the-art security mechanisms. Before a reader can begin a dialogue with a card, it uses "mutual authentication" to ensure that both the reader and card can trust each other. Only after this process occurs is the reader allowed to access the data stored inside the card. Usually this data is protected by cryptographic algorithms and secret keys so that if the data were somehow extracted, or even "spied" on, it would be very difficult to decipher and utilize.

As with 125 kHz Prox technology, contactless smart cards are convenient for users who merely present their cards near a reader. In addition, users do not have to carefully insert the card into a slot or worry about proper orientation. This also minimizes the physical wear-and-tear on both the card and the reader, the potential for vandalism, and environmental elements.

Amplifying the convenience of contactless smart cards is their capability to support more than one application at a time. For example, a single card can be used for the dual purposes of opening a door and logging on to a computer.

Contactless smart cards also provide greater and ever-increasing amounts of memory, enhancing the sophistication of applications. Enough memory is available to store biometric templates and even photos, enabling additional factors for user authentication. Such authentication of both the card and user increases the security and likelihood that the person using the card is indeed the authorized user of that card.

Different Security for Different Cards

There are different levels of security offered by commonly used card technologies in the access control marketplace. Figure 1 rates the relative "strength" of each card technology based on the availability of information required to illegally read or copy it -- the higher the number, the more secure the technology.

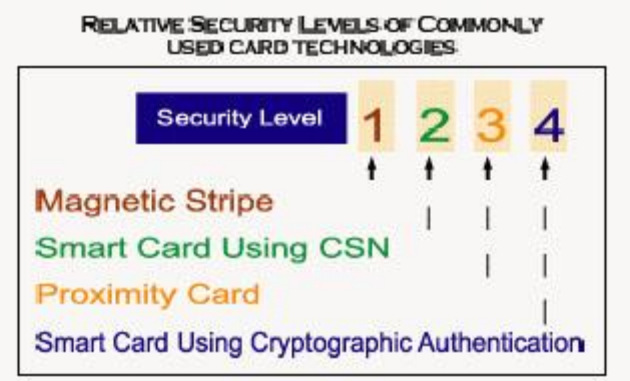
RELATIVE SECURITY LEVELS OF COMMONLY USED CARD TECHNOLOGIES
Security Level
1
2
3
4
Magnetic Stripe
Smart Card Using CSN
Proximity Card
Smart Card Using Cryptographic Authentication

Figure 1. Relative security levels of commonly used card technologies (lowest of highest) (Source : HID Global Corporation)

Magnetic Stripe has the lowest security because it is well-documented by ISO standards[1] and it typically uses little or no security protections. As important, off-the-shelf devices are widely available to encode cards. Using the CSN of a contactless smart card is also low security because it is also well-documented by ISO standards and there is no secure authentication of the CSN. A significant amount of CSN emulation activity has been reported and off-the-shelf devices to mimic or clone the CSNs of cards are now available.

Prox Cards, on the other hand, offer higher security than the practice of using the CSN of contactless smart cards because information about Prox technology is not well documented nor is it the subject of any ISO specifications; and every Prox manufacturer uses its own methods to encode and protect data.

Contactless smart cards, when properly implemented and deployed, offer the highest security and interoperability. These cards use mutual authentication and employ cryptographic protection mechanisms with secret keys. They may also use special construction and electrical methods to protect against external attacks.

[1] http://en.wikpedia.org/wiki/Magnetic_stripe

A False Sense of Security

To understand why using the serial number of contactless smart cards provides a false sense of security, it is first important to understand some basic definitions and contactless smart card mechanisms.

• CSN

CSN refers to the unique serial number of a contactless smart card. All contactless smart cards contain a CSN as required by the ISO specifications 14443[2] and 15693[3]. CSNs are typically 32 to 64 bits long.

The CSN goes by many other names including UID (Unique ID), PUPI (Pseudo Unique Proxcard Identifier), CUID (Card Unique ID), and of course CSN (Card Serial Number). It is important to note that the CSN can always be read without any security or authentication as per the ISO requirements.

Think of the CSN using the analogy of the identifying number on a house. It is important for everyone to be able to read the house number to find you. Similarly, the CSN is used to uniquely identify a card when more than one card is presented at a reader at the same time. Moreover, nobody can get in to your house or get in to a smart card without using the correct key.

[2] http://en.wikipedia.org/wiki/ISO_14443_14443

[3] http://en.wikipedia.org/wiki/ISO_15693_15693

● Anticollision

Anticollision is part of the protocol used by contactless smart cards to uniquely identify a card when more than one card is presented at a reader at the same time. It provides the ability to communicate with several contactless smart cards simultaneously. This is especially important in long-range readers, as illustrated by Figure 2.

Figure 2. Illustration of anticollision (Source : HID Global Corporation)

The ISO standards require that every contactless smart card have a unique CSN and these standards describe several methods to implement anticollision. It must be pointed out that the CSN was never intended by ISO to be used for any purpose other than anticollision.

CSN for Access Control

CSN readers are readers that use the CSN of a contactless smart card instead of the credential data stored in the secure area of the card. When a card is presented to the reader, it reads the CSN and typically extracts a subset of the CSN, converts it to a 26-bit Wiegand or other output format, and then outputs this data to an upstream device such as a panel or host computer.

● Intensifying the Problem

Most readers used for access control applications transmit their data using the Wiegand protocol[4]. This protocol is both an electrical interface and a data content protocol. The data content of the Wiegand protocol is referred to as a "format" There are many formats available and formats are comprised of multiple "fields" The most commonly used format contains a total of 26-bits and includes a site code field (8-bits), a card number field (16-bits), and two parity bits.

The site code field (also called a facility code) is usually the same for all cards at a given site and is used to ensure that cards from different facilities in the same geographic area can be distinguished from each other. Without this field, cardholders with the same card number might be able to access facilities for which they do not have authorization. The card number field uniquely identifies each cardholder and the parity bits are used to detect data communication errors.

If the 26-bit Wiegand protocol is being used, the 16-bit card number field is extracted from the CSN and the site code field is usually created from a pre-programmed number stored in the reader. Because the smart card manufacturer preprograms the CSN, using only a small portion of the CSN introduces the likelihood that there will be duplicate card numbers. Statistically, out of every 65,535 cards, there will be at least one duplicate. This is why it is desirable to use a Wiegand format with more bits in the card number field.

Keep in mind that the issue of duplicate card numbers is not limited to the Wiegand protocol. It occurs in any protocol that uses a reduced number of bits from the CSN.

4)SIA AC-01-1996. 10, http://webstore.ansi.org/ansidocstore/dept.asp=3117

● Sacrificing Security

To create a low-cost "universal" reader capable of reading any manufacturers contactless smart card, reading the CSN is the easiest, and sometimes the only, way to achieve interoperability. One or more of the following reasons are at the heart of the problem:

1. The inclusion of the hardware chip containing the security algorithms adds cost.
2. The reader manufacturer may have to pay a hefty license fee for the security algorithms or the reader manufacturer may not be able obtain a license.
3. The security keys to the contactless smart cards are not available.

Using a low-cost "universal" reader that does not avail itself of the security features that contactless smart cards offer will compromise the security of the facility or area where it is used. As noted earlier, the three major reasons to use contactless smart cards are security, convenience, and interoperability. Figure 3 illustrates how using the CSN compromises these three key reasons.

● Getting Inconvenient & Expensive

CSNs are non-consecutive numbers that are in a random order. Therefore, referring to a cardholder by its CSN makes it impossible to group employees by card number ranges such as 1-100.

Furthermore, as discussed above, it is desirable to use all of the bits required to represent the entire CSN. A 32-bit CSN would be represented as a number with as many as 10 digits and a 64-bit CSN requires as many as 20 digits. Even using the hexadecimal notation to enter CSNs still requires a person to type up to 16 characters to add or change a card.

With an enrollment reader, the process of adding cards to a system can be simplified since the CSN of a card can be read instead of being typed. However, this introduces more complexity to the system, requiring additional access control software and hardware. Moreover, if a cardholders privileges have to be changed, an enrollment reader is of no use when the card is not available.

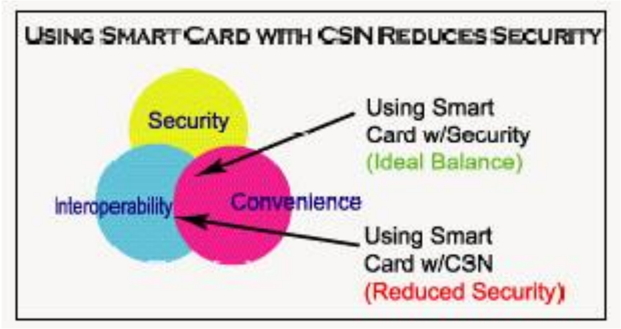

Figure 3. Using smart card with CSN reduces security. (Source : HID Global Corporation)

● Compromising Privacy

Because reading only the CSN of a contactless smart card requires less power, read distances are often greater. This is because the power-hungry cryptography circuitry inside the contactless smart card is not used. Greater read distances, coupled with no authentication or security, make the cards far less secure from illegal activities at even greater distances.

In addition, using the CSN gives the false impression that a particular readers performance is greater than it actually is. This may be doubly misleading for users because the CSN reader may be less expensive and offer better read distances than a reader that fully implements the security protections available with contactless smart card technology.

● Official Recommendations

A US Government report[5] recommends not using the CSN for identification purposes since "…using the CSN as a unique identifier works only for 14443A, and for 14443B it [may] be a random number that changes every time and will be discussed in a future version of the specification."

The International Civil Aviation Organization[6] also warns, "There is no protection in use of a CSN because this is often set in software by chip manufacturers and can be changed."

[4] SIA AC-01-1996. 10, http://webstore.ansi.org/ansidocstore/dept.asp?dept_id=3117=3117

[5] "Common Access Card Pre-Issuance Tech Requirements v4.1.2 w/9/05", http://www.icao.mrtd/down

[6] Annex K of ICAO NTWG Biometrics Deployment Technical Report, International Civil Aviation Organization(ICAO), page 19, http://www.icao.int/mrtd/down

● Expert Opinions

Both cryptographers and industry experts also warn of the dangers of using the CSN to identify a cardholder. David Engberg of Corestreet Ltd.[7] says, "The serial number has no cryptographic or protocol-level protections to prevent an attacker from asserting the same serial number as any real card. By implementing ISO 14443 directly, an attacker can imitate any desired CSN."

Bruno Charrat, CTO of Inside Contactless[8)], concurs with David Engberg, adding, "As soon as there is no security in the communications, you can clone a card and then enter anywhere you want! It is as simple as that."

Giesecke & Devrient GmbHs Klaus Finkenzeller[9)] agrees saying, "Yes, it is true! In general, almost all contactless smart cards using programmable microprocessors with an OS can change their CSN."

Greg Young, Technical Sales Manager for RFI Communications & Security Systems, warns against the assumption that contactless smart cards offer more secure transmission than Prox cards. "They can be more secure, but theyre not necessarily more secure," he said. "Many manufacturers are touting readers that read multiple types of smart card technology -- MIFARE, iCLASS -- when really all theyre reading is the serial number sent unencrypted from the card, in the same way Prox is. Unless you make sure that what youre reading is from a secure sector on the card that can be truly encrypted, and there is a handshake procedure between the reader and the card before transmission, what youre getting is no more secure than proximity technology."

7)"Secure Access Control with Government Contactless Cards, David Engbeg, Corestreet Ltd.", Cambridge, MA, http:/http://www.rfid-handbook.de/english/index.php

8)Bruno Charrat, CTO, Inside Contactless Aix-en-Provence, France, www.insidecontactless.com

9)Klaus Finkenzeller, Giesecke & Devrient GmbH, http://www.rfid-handbook.de/english/index.php

Refuting Commonly Held CSN Beliefs

● What about Encrypted CSNs?

Encrypted CSNs offer no real protection from cloning and replay attacks.

● What about Random CSNs?

The ISO specifications state, "The CSN is a fixed unique number or a random number which is dynamically generated by the contactless smart card." Finkenzeller, author of the "RFID Handbook" [10)], explains, "In contrast to type A cards, the serial number of a type B card is not necessarily permanently linked to the microchip, but may even consist of a random number, which is newly determined after every power-on reset."

Clearly, using a CSN reader with contactless smart cards that utilize random CSNs cannot work. Every time the cards are presented to the reader, their CSNs would be different.

10)RFID Handbook, Klaus Finkenzeller, http://www.rfid_handbook.de/english/index.html

● Chips with Programmable CSNs

The statement -- The CSN is a unique serial number permanently written into the device? nonvolatile memory at the factory; it cannot be modified and is guaranteed to be unique for all devices.-- is not always true.

Some contactless smart cards have programmable CSNs but there is no guarantee of the authenticity of a CSN and CSN readers compromise security.

Best Use of CSN Readers

CSN readers are very useful as a temporary solution to migrate from one smart card manufacturer to another. A single reader can be used to read both the existing cards using its CSN and the new replacement cards using full security and authentication. This provides a window of time to replace the cards. When all of the existing cards have been replaced, the reader can then be instructed to turn off its CSN reading capability. For maximum security, it is best to keep the replacement time period as short as possible.

Using the CSN for anything other than its intended use severely reduces the security of a contactless smart card. In other words, CSN is really an acronym for Compromisable Serial Number. When implementing and deploying contactless smart card technology, always consider the following:

1. Contactless smart cards are very secure when used properly.
2. Using the CSN of a contactless smart card bypasses the security built into smart cards.
3. Prox offers greater security than using the CSN of contactless smart cards.

Understanding the security risks associated with using the CSN instead of reading the data protected by security mechanisms will help ensure that the proper protections are in place for both personnel and property.