HID Global: contactless smart cards - dumb (and dangerous) ways to use them - Part I

HID Global: contactless smart cards - dumb (and dangerous) ways to use them - Part I. 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’s serial number (CSN). This provides a false sense of security analogous to installing a high security door without any locking mechanism – says Michael L. Davis, Director of Technology–Intellectual Property, HID Global Corporation.

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.

Why Use Contactless Smart Cards?

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.

**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** 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 and 15693.

CSNs are typically 32 to 64 bits long. It is important to note that the CSN can always be read without any security or authentication as per the ISO requirements.

**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.

**How is a CSN Used 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.

To create a low-cost “universal” reader capable of reading any manufacturer’s 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: The inclusion of the hardware chip containing the security algorithms adds cost - if they are at all available.

The reader manufacturer may also have to pay a hefty license fee for the security algorithms or the reader manufacturer may not be able obtain a license.

Part II will be published in the next issue of GIT SECURITY + MANAGEMENT

Contact:

**HID Global,**
Haverhill, United Kingdom
Tel.: +44 1440 714 850
Fax: +44 1440 714 840
infoEMEA@hidcorp.com
www.hidcorp.com