Dangers of CSN-only Smart Card Readers

A false sense of security can leave you more vulnerable than you know

Introduction

When contactless smart cards are implemented and deployed properly, they represent one of the most secure identification technologies available. However, some manufacturers, in an attempt to sell a 'universal' reader capable of reading almost any contactless smart card technology, actually disable the built-in security mechanisms. These readers, referred to as 'CSN readers', only read the card's serial number which, per ISO standards, is not be protected by any security. The ISO standard specifies use of the CSN for a process referred to as anti-collision, which is designed only to identify more than one distinct card in the field of the reader, and does not include security measures. An understanding of these details can allow a perpetrator to build a device to clone (or simulate) the CSN of a contactless smart 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 important to understand some basic definitions and contactless smart card mechanisms.

Card Serial Number (CSN): CSN refers to the unique card serial number of a contactless smart card. All contactless smart cards contain a CSN as required by the ISO specifications 14443and 15693. The CSN goes by many other names including UID (Unique ID), and CUID (Card Unique ID). *It is important to note that the **CSN can always be read without any security or authentication per ISO requirements.***

In addition, there are smart card development tools such as protocol analyzers that are widely available and can emulate an ISO 14443 or 15693 CSN.

It's helpful to 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 it. Similarly, the CSN is used to uniquely identify a card.

Anticollision: Anticollision is part of the communications 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.

ISO standards require that every contactless smart card have a unique CSN and these standards describe several methods to implement anti-collision. *It is important to note that the **CSN was never intended by ISO to be used for any purpose other than anticollision.***

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 a reader, it reads the CSN and typically extracts a subset of the CSN, converts it to a 26-bit Wiegand or other

unsecure output format, and then outputs this data to an upstream device such as a control panel or host computer.

Most Commonly Used Card Format Intensifies the Problem
There are many card formats available and formats are comprised of multiple fields. The most commonly used card format contains a total of 26-bits.

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. This introduces the likelihood that there will be duplicate card numbers. Statistically, out of every 65,535 cards, there will be at least one duplicate.

It is best practice to use a card format with more bits in the card number field. Some manufacturers offer a card format that uses both a larger card number field and includes an additional customizable field together with the site code 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 derived from the CSN to represent a card number.

If these issues with security are so obvious, why is CSN reading so popular?
Providers who seek to provide the lowest cost product, often choose not to pursue proper licensing of the security algorithms to minimize their costs. They also often fail to educate their customers on the compromise they are introducing into the customer's security solution. While the customer may benefit from a low price at install, the long term cost of a security compromise can be catastrophic.

Recommendations from Government and International Organizations
The U.S. Government and International organizations warn against the use of CSN other than its intended use.

- A U.S. Government report 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 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."

Summary
When implementing and deploying contactless smart card technology, use best practice and always consider the following:

- Contactless smart cards are secure when used properly
- Using the CSN of a contactless smart card bypasses the security built into 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.

2016-09-19-hid-dangers-of-csn-eb-en PLT-03093