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

HID Global: contactless smart cards - dumb (and dangerous) ways to use them - Part II. 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. This is the second and last part of Michael L. Davis’ thoughts on the right use of contactless smart cards.

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, 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 cardholder’s privileges have to be changed, an enrollment reader is of no use when the card is not available.

Using CSN Can Decrease Privacy

Because reading only the CSN of a contactless smart card requires less power, read distances are often greater. This is because the powerhungry 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 reader’s 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.

When Should a CSN Reader Be Used?

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.

Conclusion

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.
InfoSecurity Europe, Stand H164

Contact: