



Zagrożenia związane z używaniem bazujących wyłącznie na numerze CSN

Falszywe poczucie bezpieczeństwa może być groźniejsze, niż się wydaje.

Wprowadzenie

Właściwie wdrożone i stosowane inteligentne karty zbliżeniowe są jedną z najbezpieczniejszych dostępnych obecnie metod identyfikacji. Jednak niektórzy producenci, chcąc sprzedawać „uniwersalne” czytniki zdolne obsługiwać niemal wszystkie technologie inteligentnych kart zbliżeniowych, de facto rozbrajają ich wbudowane mechanizmy zabezpieczające. Czytniki takie – zwane czytnikami CSN – rozpoznają jedynie numer seryjny karty, który zgodnie ze standardami ISO nie jest w żaden sposób zabezpieczony. Standard ISO definiuje wykorzystywanie numeru CSN wyłącznie w ramach procesu antykolizyjnego, tj. procesu umożliwiającego rozpoznanie właściwej karty, gdy w zasięgu czytnika znajdzie się ich kilka. Sam w sobie numer ten nie jest jednak w żaden sposób zabezpieczony. Dysponując wiedzą na ten temat, przestępca może stworzyć urządzenie do klonowania (lub podrabiania/symulowania) numerów CSN inteligentnych kart zbliżeniowych.

Falszywe poczucie bezpieczeństwa

Aby zrozumieć, dlaczego używanie numeru seryjnego inteligentnej karty zbliżeniowej daje fałszywe poczucie bezpieczeństwa, należy poznać podstawowe definicje i sposób działania takiej karty.

Numer seryjny karty (CSN): CSN to unikalny numer seryjny inteligentnej karty zbliżeniowej. Zgodnie ze standardami ISO 14443 i 15693 każda inteligentna karta zbliżeniowa musi mieć numer CSN. Jest on również znany jako UID (Unique ID – unikalny identyfikator) czy CUID (Card Unique ID – unikalny identyfikator karty). *Należy pamiętać, że zgodnie z wymogami ISO numer CSN można zawsze odczytać bez konieczności pokonywania jakichkolwiek zabezpieczeń czy stosowania uwierzytelnienia.*

Co więcej na rynku powszechnie dostępne są narzędzia dla projektantów kart inteligentnych, np. analizatory protokołów, które umożliwiają emulację numeru CSN zgodnego ze standardem ISO 14443 lub 15693. Numer CSN można porównać do numeru umieszczonego na budynku. Każdy powinien móc go łatwo odczytać, aby dotrzeć pod szukany adres. Numer CSN umożliwia natomiast precyzyjną identyfikację karty

Mechanizmy antykolizyjne: Mechanizm antykolizyjny jest częścią protokołu komunikacyjnego używanego przez inteligentne karty zbliżeniowe do pewnej identyfikacji konkretnej karty, gdy do czytnika zostanie w tym samym momencie zbliżonych wiele kart. Mechanizmy te umożliwiają jednoczesne komunikowanie się czytnika z kilkoma inteligentnymi kartami zbliżeniowymi.

Zgodnie ze standardami ISO każda inteligentna karta zbliżeniowa powinna mieć swój unikalny numer CSN. Standardy ISO opisują też kilka różnych metod wdrażania mechanizmu antykolizyjnego. Należy podkreślić, że *standardy ISO nigdy nie przewidywały stosowania numeru CSN w celu innym niż prowadzenie procesów antykolizyjnych.*

W jaki sposób numer CSN jest używany przy kontroli dostępu?

Czytniki CSN rozpoznają inteligentną kartę zbliżeniową na podstawie numeru CSN, a nie na podstawie danych poręczeń zapisanych w bezpiecznym sektorze karty. W momencie zbliżenia karty czytnik rozpoznaje numer CSN i zazwyczaj wyodrębnia jego podzbiór, po czym konwertuje go na 26-bitowy format Wiegand lub na inny niezabezpieczony format wyjściowy. Następnie przesyła te dane do urządzenia nadrzędnego takiego jak panel sterowania czy komputer główny.

Najpowszechniej stosowany format kart przyczynia się do narastania problemu.

Istnieje wiele formatów kart, a każdy z nich składa się z różnej liczby pól. Najpopularniejszy jest format 26-bitowy. W przypadku użycia 26-bitowego protokołu Wiegand z numeru CSN wyodrębniane jest 16-bitowe pole numeru karty. Następnie – najczęściej na podstawie przechowywanego w czytniku wstępnie zaprogramowanego numeru – tworzone jest pole kodu lokalizacji. Takie rozwiązanie rodzi możliwość wystąpienia zduplikowanych numerów kart. Statystycznie na każde 65 535 kart przypada co najmniej jeden duplikat. Dlatego zalecane jest stosowanie formatu z większą liczbą bitów w polu numeru karty. Niektórzy producenci oferują format, który oprócz większego pola numeru karty zawiera też pole dodatkowe z możliwością jego indywidualnego dostosowania oraz pole kodu lokalizacji. Warto pamiętać, że problem duplikowania numerów kart występuje nie tylko w przypadku protokołu Wiegand. Dotyczy on *każdego* protokołu, który przedstawia numer karty za pomocą ograniczonej liczby bitów pobranych z numeru CSN.

Dlaczego mimo oczywistych problemów z zabezpieczeniami czytniki CSN są tak popularne?

Dostawcy, chcąc zaoferować jak najtańszy produkt, często rezygnują z właściwie licencjonowanych algorytmów bezpieczeństwa, aby obniżyć koszty. Często też nie informują klientów o tym, że wdrażane rozwiązanie może stworzyć lukę w systemie zabezpieczeń. Choć niska cena przy instalacji wydaje się klientom atrakcyjna i korzystna, długofalowy koszt związany z naruszeniem bezpieczeństwa systemu może okazać się katastrofalnie wysoki.

Rekomendacje wydane przez rządy i organizacje międzynarodowe

Rząd Stanów Zjednoczonych i organizacje międzynarodowe ostrzegają przed używaniem numeru CSN w sposób niezgodny z jego przeznaczeniem.

- Raport rządu USA zaleca, by nie używać numeru CSN do identyfikacji, ponieważ „... używanie numeru CSN jako unikalnego identyfikatora działa tylko w przypadku standardu 14443A, natomiast w przypadku standardu 14443B może być to losowy numer zmieniający się za każdym razem – rozwiązanie to zostanie omówione w kolejnej wersji specyfikacji”.
- Międzynarodowa Organizacja Lotnictwa Cywilnego ostrzega też, że „numer CSN nie gwarantuje bezpieczeństwa, ponieważ jest często definiowany w oprogramowaniu przez producentów układów scalonych i możliwy do zmiany”.

Podsumowanie

Przedsiębiorstwa planujące wdrożyć i stosować technologię inteligentnych kart zbliżeniowych powinny skorzystać z najlepszych praktyk rynkowych i zawsze pamiętać o tym, że:

- Inteligentne karty zbliżeniowe są w pełni bezpieczne, o ile używa się ich we właściwy sposób;
- Stosowanie numeru CSN inteligentnej karty zbliżeniowej polega na omijaniu funkcji zabezpieczeń wbudowanych w kartę.

Aby właściwie chronić pracowników i mienie, należy zdawać sobie sprawę z ryzyka płynącego z zastąpienia odczytu danych chronionych przez mechanizmy zabezpieczające metodą identyfikacji przy użyciu numeru CSN.

© 2016 HID Global Corporation/ASSA ABLOY AB. Wszelkie prawa zastrzeżone. HID, HID Global, logo HID Blue Brick i Chain Design to znaki towarowe lub zarejestrowane znaki towarowe firmy HID Global lub jej licencjodawców/dostawców w Stanach Zjednoczonych i/lub innych krajach. Zabrania się używania ich bez pozwolenia. Wszystkie inne znaki towarowe, znaki usługowe oraz nazwy produktów i usług stanowią znaki towarowe lub zarejestrowane znaki towarowe swoich właścicieli.
2016-09-19-hid-dangers-of-csn-eb-pl PLT-03123