

# Pericole suplimentare ale permiselor de conducere electronice

## 1) Citirea datelor cu caracter personal într-un mod extrem de facil

Spre deosebire de cipurile RFID din pasapoarte, cele din permisele de conducere nu posedă nici un fel de sistem de criptare a datelor. Ele pot fi accesate de orice cititor compatibil cu frecvența dispozitivului. Orice infractor își poate procura un astfel de cititor la un pret de circa 200 de euro. Adăugându-i o antena performantă - de asemenea ușor de procurat la un pret mic - poate începe să scaneze datele celor care circulă pe stradă, dacă au asupra lor carnetul de conducere. Orice sofer este potențială victimă.

## 2) Citirea datelor cu caracter personal folosind dispozitive compatibile GSM

Spre deosebire de cipurile RFID din pasapoarte, cele din permisele de conducere funcționează la o frecvență înaltă (900 MHz) compatibilă cu cea GSM (GSM-900). Deci, anumite telefoane mobile pot fi modificate și folosite ca scannere improvizate (dar eficiente) pentru astfel de cipuri. Distanța de citire este și ea, se înțelege, mult mai mare (anumite teste avansează distanțe extrem de mari, de ordinul sutelor de metri). Inutil să spunem că mână cerească reprezintă aceste lucruri pentru rețelele de crimă organizată și/sau spionaj. Presupunând că un om nu poartă tot timpul pasaportul la el (decât atunci când calătorește), permisul de conducere îl poartă aproape sigur mai tot timpul la el. Toate problemele prezente la pasapoarte se echivalează și în cazul permiselor, cu mențiunea că acestea sunt MULT mai ușor de urmărit și accesat decât pasapoartele.

LUCIAN CORNIANU,  
Președinte ACESDS, Inginer fizician, Inginer de sistem

# Pericolele pasapoartelor electronice

## 1) Citirea datelor cu caracter personal (nume, prenume, CNP, naționalitate, vârsta etc.)

Aceste date pot fi folosite pentru deschiderea unor conturi bancare. Pot fi folosite, de asemenea, pentru achiziționarea de proprietăți, derularea de licitații electronice, înființarea unor societăți comerciale fantomă. Toate acestea, în scopul defășurării unor activități ce implică spălarea de bani, escrocherie, crimă organizată, terorism și altele asemenea. Dat fiind că datele folosite sunt ale dumneavoastră, deci date reale, pe de-o parte tranzacțiile vor decurge ușor, falsul fiind greu de descoperit, iar pe de altă parte nu veți putea dovedi că altcineva a făcut aceste lucruri decât extrem de greu și de încet (în unele cazuri, deja întâlnite în SUA la furturile de identitate, victima va fi în puscărie înainte să-și poată dovedi nevinovăția și va avea nevoie de ani de zile pentru a ieși - cu o viață distrusă).

## 2) Citirea datelor cu caracter biometric (amprenta digitală, amprenta facială, amprenta retinei)

Pot fi folosite pentru clonarea amprentelor digitale și amprentelor de retina (lentile de contact personalizate). Pot fi folosite pentru a avea ulterior acces la anumite informații securizate ale persoanei respective sau la locul de muncă al acesteia (multe calculatoare și instituții folosesc genul acesta de control al accesului). Pot fi folosite pentru plantarea de probe false la locul unei infracțiuni, în special a amprentelor, care sunt cel mai ușor de clonate (pe suport de latex). Pot fi folosite pentru confecționarea de masti personalizate sau trucare de înregistrări de imagini - adăugându-se amprenta dumneavoastră facială la locul comiterii unei infracțiuni.

### **3) Clonarea cipurilor, modificarea datelor si atasarea lor la un alt pasaport**

Clonarea înseamna citirea datelor de pe un cip, urmata de scrierea lor, în aceeasi forma, pe alt cip si atasarea acestui nou cip la un alt pasaport. Nu trebuie (neaparat) sa fie modificate datele de pe cipul original (desi se poate face asta, iar adevaratul posesor al datelor poate fi transformat în „infractor”). Modificarile pot fi facute pe cipul “clona”, care urmeaza sa fie atasat la pasaportul fizic falsificat în prealabil (sau pur si simplu cumparat de la firma producatoare - legal sau nu - cu un cip fara date). Se înțelege ca în felul acesta falsul este aproape imposibil de detectat, pasaportul fiind declarat 100% valid de catre cititorul RFID, singura speranta ramânând, ca si pâna acum, în ochiul vigilent al vamesului. Daca datele sunt clonate pe un pasaport original cumparat pe sub mâna - lucru usor de facut în orice tara în care exista coruptie - atunci falsul nu poate fi descoperit decât cu totul exceptional. Victima nu va avea nici o sansa sa se justifice în libertate, odata ce infractiunile au fost comise de purtatorul unui asemenea pasaport. Va intra în închisoare si va trebui sa adune dovezile nevinovatiei sale de acolo. Viata sociala îi va fi distrusa, cariera, de asemenea. Problema cea mai grava este ca aceste falsuri vor putea fi facute cu datele reale ale unei persoane. Pâna acum, macar falsurile se faceau cu date personale la rândul lor false, care puteau fi mai usor detectate.

### **4) Urmărirea individului purtator de act electronic cu cip**

Cipul pasaportului se identifica printr-un numar unic ce tine de tara din care provine. Chiar daca datele personale de pe pasaport nu pot fi accesate decât de la distante relativ mici, cipul poate fi scanat dupa acest ID unic de la distante extrem de mari. Oficial, cipul poate fi accesat în bune conditii de la distanta de minimum 10 cm. Asta înseamna ca el are o “dimensiune” radio sferica, având un diametru minim de 20 cm. Cel mai mic obiect care poate fi oficial interceptat fizic de un satelit civil aflat pe o orbita joasa este de 30 cm. Un satelit militar depaseste cu mult aceasta performanta. Deci, posesorul unui pasaport cu un anumit ID poate fi identificat si urmarit prin satelit.

Persoanele purtatoare de pasaport cu un anumit ID national pot astfel deveni extrem de usor tinta unor atentate teroriste punctuale. Pot fi realizate, de pilda, atacuri teroriste cu bomba sau arme chimice plasate în anumite containere, în aeroporturi, si care sa nu se declanseze decât în momentul în care pe lângă locul respectiv trece un purtator (sau un grup de purtatori) de pasaport electronic dintr-o anumita tara. De asemenea, retelele de spionaj pot beneficia din plin de aceste neajunsuri în activitatile lor curente.

### **5) Sustragerea datelor personale si biometrice din bazele de date Schengen**

Oficial, datele din noile pasapoarte biometrice urmeaza sa fie centralizate într-o baza de date unica la nivel european, cu terminale în toate statele membre Schengen. Auditul de securitate pentru aceasta baza nu a fost facut niciodata public. Atâta vreme cât servere cu lunga traditie (NASA, Pentagon etc.) cad victime periodic atacurilor informatice de tot felul, nu avem nici un motiv sa credem ca baza I si II, atât de atragatoare pentru crima organizata si pentru alte activitati infractionale, va reprezenta o exceptie. Odata ajunse pe mâinile retelelor de crima organizata, esantioanele de date biometrice vor putea fi folosite în modurile aratate mai sus pentru a crea un adevarat haos infractional si social. Recuperarea acestor date va fi practic imposibila, ele putând fi transmise în câteva clipe în orice colt al lumii. Oamenii ale caror date biometrice au fost furate nu vor mai putea niciodata sa aiba o viata linistita. Daca privim datele biometrice ca pe o cheie a identitatii personale, sa nu uitam ca aceasta cheie nu poate fi schimbata. Daca datele biometrice au fost furate, nu pot fi înlocuite în niciun fel si mereu vor aparea noi si noi incidente, accidente, contraventii si infractiuni pentru care omul ale carui date au fost furate va trebui sa se justifice. Perspectiva este limpede si îngrozitoare: milioane de vietii distruse de introducerea actelor electronice!

Permisele de conducere cu cip propuse pentru România contin si urmatoarele **pericole suplimentare fata de pasapoartele electronice:**