



Gegevens uit RFID chip van het nieuwe paspoort zijn uit te lezen

In de nieuwsbrief van september 2006 is een vorm van identity theft: pretexting aan de orde gekomen. In deze nieuwsbrief zal een andere vorm worden besproken. Het kopiëren van gegevens uit de RFID chip van het nieuwe paspoort.

Onlangs hebben onderzoekers ontdekt dat het mogelijk is om gegevens uit de RFID chip van het engelse paspoort uit te lezen.

Hierbij werd gebruik gemaakt van een simpele lezer die voor enige honderden euro's te koop is. Om de gegevens van de chip te lezen moet een encrypted sessie worden gestart. De sleutel voor deze sessie ligt echter "onder de mat". De sleutel is opgebouwd uit paspoortnummer, geboortedatum van de houder en de geldigheidsdatum van het paspoort. Deze gegevens staan ook in het gedeelte van het paspoort wat voor machines is te lezen. Hierdoor kan een machine, bijvoorbeeld aan de grens vervolgens een encrypte verbinding opzetten met de RFID chip en de gegevens uitlezen. De gegevens zelf op de chip zijn niet encrypt. De encrypte verbinding wordt opgezet om mee te lezen te voorkomen.

Het Britse ministerie van binnenlandse zaken heeft lakoniek op deze onthullingen gereageerd. Gesteld wordt dat je dezelfde gegevens ook kan lezen in het paspoort en wat moet een crimineel of terrorist nu met het digitale image van iemand?

Hier valt wel wat tegen in te brengen. Als de gegevens van de chip uit zijn te lezen, is het ook mogelijk om deze gegevens te kopiëren op een andere chip.

Lukas Grunwald, oprichter van DN-Systems Enterprise Solutions in Duitsland deed een vergelijkbaar onderzoek naar een Duits biometrisch paspoort en slaagde erin de gegevens te klonen. Dit lijkt zeker interessant voor criminelen en terroristen.

Leuk geprobeerd misschien, maar hoe kom je met een paspoort met gecloonde chip langs de gezichtsherkenner? Op de meeste vliegvelden is deze apparatuur nog niet in werking en bovendien geeft deze apparatuur nog 20 tot 25% false positives.

Het is overigens niet mogelijk om een nieuw digital image van een ander persoon aan een gecloonde chip toe te voegen. Het gecloonde paspoort kan dus alleen worden gebruikt door iemand die (enigzins) op de persoon lijkt van wie het paspoort is gekloond.

Zolang er geen (betrouwbare) gezichtsherkenners zijn is de kans klein dat iemand met een enigzins gelijkende foto en een nieuw veilig paspoort er uit wordt gehaald.

De volgende vraag is natuurlijk hoe iemand ongemerkt een RFID chip kan uitlezen. Volgens de specificatie kan een RFID chip slechts van een maximale afstand van 2 cm worden uitgelezen. Dit zou dus moeten worden opgemerkt door het slachtoffer, die vervolgens aangifte zal doen.

Nederlandse onderzoekers beweren dat het mogelijk was om de gegevens van de chip over 30 cm uit te lezen. Het zou dus mogelijk moeten zijn om naast het slachtoffer te gaan zitten en de gegevens uit te lezen.

Probleem is dat je dan nog steeds niet de juiste gegevens hebt (paspoortnummer, geboortedatum en geldigheidsdatum) om te kunnen lezen, zonder in het paspoort te kijken als het gaat om een willekeurig slachtoffer. Echter, een meer geplande aanval heeft zeker een goede kans van slagen. Het is duidelijk dat het nieuwe biometrische paspoort lang zo veilig niet is als wordt beweerd en dat identity theft zeker tot een reële mogelijkheid behoort.



Secure Connection is verhuisd

Secure Connection is onlangs verhuisd. In het geval u ons nieuwe adres nog niet heeft:

Secure Connection BV
Verlengde Poolseweg 34-46
4818 CL Breda
Tel: +31 76 5245 083
Fax: +31 76 5246 666

Actueel

Wachtwoordlek in Firefox.

De Mozilla Foundation heeft onlangs een lek gepubliceerd in Firefox 2.0. Het gaat om het stelen van wachtwoorden uit de wachtwoordmanager van Firefox 2.0. Indien een username en wachtwoord voor een bepaalde site in de wachtwoordmanager van Firefox wordt opgeslagen, wordt username en wachtwoord automatisch ingevuld, indien op deze site om username en wachtwoord wordt gevraagd. De passwordmanager checkt op url. Dit houdt in dat indien een phisher onder een subdomein van de bewuste url een nep inlogpagina bouwt, username en wachtwoord worden ingevuld. De phisher redirect deze informatie vervolgens naar een andere site, waardoor de phisher username en wachtwoord heeft. Vervolgens wordt de gebruiker geleid naar de echte site, zodat deze nietsvermoedend doorgaat. Een phisher heeft onder de populaire site Myspace een subdomein gemaakt: www.myspace.com\1sweetstar. Deze inlogpagina lijkt precies op de inlogpagina van Myspace. De truc werkt alleen als de phishingcode zich in hetzelfde domein bevindt als het domein vanwaar de phisher de username en wachtwoord wil stelen. Dit is bij sites als Myspace, waar gebruikers zelf HTML code kunnen uploaden geen probleem. Het advies is om voorlopig de passwordmanager van Firefox 2.0 niet te gebruiken, totdat de bug is gefixt.

Bron: www.bugzilla.mozilla.org
zoek op bug nummer 360493