SPITS (325000)
van: 11.06.2002 Pagina: 16 cm2: 46.13

KUN onderzoekt veiligheid software

NIJMEGEN — De Katholieke Universiteit Nijmegen (KUN) gaat samen met de Nederlandse organisatie voor wetenschappelijk onderzoek (NWO) bijna € 1,8 miljoen besteden aan een onderzoek naar de veiligheid en correctheid van computerprogramma's. Het onderzoek staat onder leiding van dr. B. Jacobs, leider van een Europees onderzoeksproject op het gebied van chipkaarten en vanaf 1 juli hoogleraar aan de KUN.

Het zogeheten Pionieronderzoek moet leiden tot certificering van software in veiligheidsgevoelige toepassingen zoals chipkaarten. De Nijmeegse onderzoeksgroep onder leiding van Jacobs ontwikkelt hulpmiddelen om die certificering mogelijk te maken. (KUN)


Staking bij melkfabrieken

HET FINANCIEELE DAGBLAD (66990)
van: 11.06.2002 Pagina: 4 cm2: 57.82

KUN onderzoekt voor miljoenen beveiliging pc's

■ De Katholieke Universiteit Nijmegen (KUN) gaat samen met onderzoeksfinancier NWO bijna € 1,8 mln besteden aan een onderzoek naar de veiligheid en correctheid van computerprogramma's. Het onderzoek staat onder leiding van dr. B. Jacobs, leider van een Europees onderzoeksproject op het gebied van chipkaarten en vanaf 1 juli hoogleraar aan de KUN. Het zogeheten PIONIER-onderzoek moet leiden tot certificering van software in veiligheidsgevoelige toepassingen zoals chipkaarten. De Nijmeegse onderzoeksgroep ontwikkelt hulpmiddelen om die certificering mogelijk te maken. De groep wil programma's systematisch kunnen doorzoeken op lekken. Omdat computers steeds vaker in allerlei netwerken staan en vanaf meerdere plekken programma's besturen, is beveiliging van groot belang, aldus een woordvoerder van de Nijmeegse universiteit. Het is de bedoeling dat door het onderzoek van Jacobs tevens een groep van deskundigen op het terrein van computerbeveiliging in Nederland ontstaat.


LPF schuift wél extra geld voor de zorg

TROUW (125353)
van: 11.06.2002 Pagina: 1 cm2: 166.54

Ook 'aftappen' pincode technisch goed te doen

door Gijs Moes

AMSTERDAM – Ook diefstal van de pincodes die bij bank- of giropassen horen is technisch mogelijk. Eerder werd al duidelijk dat bankpasjes eenvoudig worden nagemaakt. Pincodes 'aftappen' kan door een kleine aanpassing van de pinapparaten of met behulp van een speciale folie over het toetsenbord.

Dat zegt de Nijmeegse hoogleraar computerbeveiliging Bart Jacobs. „Het toetsenbord is het zwakke punt. Het is geen probleem om de ingetoetste code net achter het apparaat af te tappen. De banken willen hier liever niet te veel bekendheid aan geven."

Volgens de hoogleraar hebben criminelen in Groot-Brittannië al gewerkt met een speciale folie. De folie met daarin contactdraden wordt over het toetsenbord geplakt, waarna de pincode eenvoudig en doeltreffend kan worden 'afgekeken'.

Een woordvoerder van Interpay, de organisatie die namens de banken het elektronische betalingsverkeer verzorgt, erkent de mogelijkheid dat criminelen via technische middelen de pincode achterhalen. Tot nu toe hielden banken en Interpay vol dat dat onmogelijk was.

De politie in Amsterdam heeft eerder een winkelbediende aangehouden die passen kopieerde met behulp van een extra apparaat achter de toonbank. Met de nagemaakte passen werd later geld opgenomen. Justitie sluit niet uit dat dit op meer plaatsen in Nederland gebeurt.

„De informatie op de magneetstrip van pinpassen is heel gemakkelijk te kopiëren", zegt Jacobs, hoogleraar beveiliging en correctheid van programmatuur aan de Katholieke Universiteit Nijmegen. Een apparaat van ruim dertig euro is voldoende om de informatie op de magneetstrip te lezen en vast te leggen. „Het zijn gewoon domme kaarten", onderstreept hij.

Wie vervolgens de gegevens op een lege kaart à 1,20 euro zet, heeft een kopie van de bank- of giropas in kwestie, zonder dat de eigenaar iets in de gaten heeft gehad. „Dan ben je als crimineel een heel eind", erkent de woordvoerder van Interpay. De organisatie bepaalt de specificaties waar de apparaten aan moeten voldoen en de richtlijnen voor het gebruik ervan. De woordvoerder benadrukt dat de techniek zeer veilig is, „maar altijd afhankelijk van de mens".

In Engeland is het zogenoemde *skimming* inmiddels een bekend probleem. Vorige maand heeft de politie in Londen een nieuwe afdeling opgezet, met 23 medewerkers. Fraude met nagemaakte pinpassen heeft de banken daar vorig jaar al 246 miljoen euro gekost.


Trouw
Annan: Westen moet zich diep schamen
'Mariaverschijningen authentiek'
Les Bleus hebben al verloren

TROUW (125353)
van: 11.06.2002 Pagina: 5 cm2: 231.02

Imago van pinpas brokkelt snel af

De banken hebben het gebruik van pinpas en pincode altijd als zeer veilig voorgesteld. Nu blijkt dat criminelen de pas eenvoudig kunnen kraken en zelfs de pincode kunnen afkijken. En daar is vooralsnog weinig tegen te doen.

Pinpasjesfraude

Gijs Moes

Een verbod op de verkoop van een niet door Interpay gekeurde kaartlezers is lastig. Sommige bedrijven willen hun eigen beveiligings- of toegangssysteem opzetten, waar ze dit soort kastjes voor nodig hebben. Bovendien is de verkoop via internet moeilijk te controleren. Volgens Interpay is een eventueel verbod 'een zaak van justitie'. Jacobs adviseert dan ook altijd goed te kijken wat er met de bank- of giropas gebeurt. Maar volgens hem is het aflezen van de gegevens ook mogelijk als de klant zelf de pas hanteert.

Gelukkig is er nog altijd de pincode, die nodig is om met een pas geld op te kunnen nemen. Dat biedt natuurlijk beveiliging en de banken waarschuwen dan ook regelmatig de pin geheim te houden. Toch zijn er meerdere manieren om de code af te kijken. Het eenvoudigst is wel een ('behulpzame') handlanger die over de schouder meekijkt en de code onthoudt. Advies van de banken: scherm bij het intoetsen uw hand zoveel mogelijk af.

Afschermen moet ook helpen tegen een iets geavanceerdere manier van meegluren: via een camera. De camera's die bijvoorbeeld een benzinepomp vaak heeft hangen, bieden over het algemeen een veel te slecht beeld om de code af te kunnen lezen. ,,Ze zijn meestal bedoeld om een beeld van de hele zaak te geven, ook winkeldiefstal ergens in een hoek'', aldus een woordvoerder van Shell. Interpay stelt ook eisen aan de plaatsing van camera's en spiegels. Maar een kwaadwillende pombediende kan een klein cameraatje verdekt ophangen, boven het toetsenbordje.

Er is een nog veel sluwere manier om de pincode van een klant te stelen: een speciale folie, met contactdraden erin, die over het toetsenbord wordt geplakt. Op deze manier is de code eenvoudig en ongemerkt vast te stellen. Bovendien is het voorstelbaar dat criminelen het pin-apparaat openschroeven en wat draadjes aansluiten om zo de ingetoetste code af te tappen. ,,Ik kan me er wel iets bij voorstellen dat criminelen zo gegevens onderscheppen'', geeft een woordvoerder van Interpay aarzelend toe.

De producent van pinkastjes Alphyra zegt niet bekend te zijn met deze mogelijkheid. ,,De automaat belt met Interpay en verstuurt het geheel van pincode en gegevens van de pas als versleutelde informatie door'', aldus product manager A. Mulder. Volgens hem is dat een veilig proces. ,,Ik heb altijd begrepen dat het onthouden van de pincode via het toetsenbord niet mogelijk is'', aldus de Shell-zegsman.

Jacobs is minder voorzichtig: ,,Het toetsenbord is gewoon het zwakke punt. De ingetoetste code moet toch naar de bank verstuurd worden en het is maar net op welk niveau je de informatie aftapt.'' Hij begrijpt de algemene voorzichtigheid wel. ,,De banken willen hier natuurlijk liever niet teveel bekendheid aan geven.''

Ook als straks de magneetstrip vervangen is door een chip, blijft het toetsenbord een zwak punt aldus Jacobs. Een chip is volgens hem op zich wel veiliger, want veel moeilijker te kopiëren. ,,Die is zeker niet in een keer achter de toonbank te kopiëren.'' Maar ook criminelen zullen steeds nieuwe wegen vinden om de gewilde gegevens te achterhalen, erkent Jacobs. ,,Het blijft een kat-en muisspel.''


Staking in de zuivel breidt zich uit

Bezem niet rigoureus door RNV-beleggingen

DE TELEGRAAF (807800)
van: 11.06.2002 Pagina: 3 cm2: 58.57

Onderzoek naar veiligheid van computer-programma's

NIJMEGEN, dinsdag
De Katholieke Universiteit Nijmegen (KUN) gaat samen met de Nederlandse organisatie voor wetenschappelijk onderzoek (NWO) bijna 1,8 miljoen euro besteden aan een onderzoek naar de veiligheid en correctheid van computerprogramma's.

Het onderzoek staat onder leiding van dr. B. Jacobs, leider van een Europees onderzoeksproject op het gebied van chipkaarten en vanaf 1 juli hoogleraar aan de KUN.

Het zogeheten PIONIER-onderzoek moet leiden tot certificering van software in veiligheidsgevoelige toepassingen zoals chipkaarten. De Nijmeegse onderzoeksgroep onder leiding van Jacobs ontwikkelt hulpmiddelen om die certificering mogelijk te maken. (ANP)


Nieuw kabinet komt met vrijstelling ozb