TWOBESMART:

MULTIFUNCTIONELE SMARTCARDS VOOR TOEGANGSVERLENING

DRS. V.W. STINESEN

ptt research

DE CONCERNSTAVEN BEDRIJFSVEILIGHEID EN INFORMATIEMANAGEMENT VAN PTT HEBBEN GECONSTATEERD DAT DE TOEGANGSBEVEILIGING BIJ KONINKLIJKE PTT NEDERLAND NV VERBETERD KAN WORDEN. UIT ONDERZOEK VAN PTT RESEARCH IS GEBLEKEN DAT HUIDIGE MIDDELEN, ZOALS DE MAGNEETSTRIPKAART EN DE USERID-PASSWORD COMBINATIE, QUA BEVEILIGING TE KORT SCHIETEN. DE MAGNEETSTRIPKAART IS OP EENVOUDIGE WIJZE TE KOPIEREN EN GEBRUIKERS VAN USERID-PASSWORD COMBINATIES SPRINGEN ERG ONZORGVULDIG MET HUN PASSWORDS OM. ZE KIEZEN EENVOUDIG TE ACHTERHALEN PASSWORDS OF NOTEREN DE PASSWORDS.

Uit hetzelfde onderzoek blijkt dat smartcards goede mogelijkheden bieden om de tekortkomingen op te heffen. Daarom hebben de genoemde concernstaven PTT Research de opdracht gegeven om de logische en fysieke toegangsbeveiliging bij PTT te optimaliseren en de smart card op haar merites te beoordelen.

smartcards

Een smartcard is een plastic kaartje met de afmetingen van een credit card waarin een kleine computer geplaatst is.

De smartcard heeft onder meer de volgende specifieke eigenschappen:

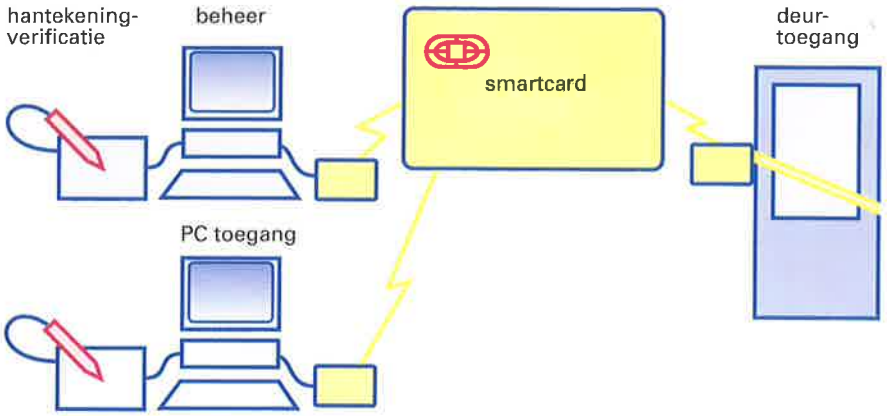
- het geheugen van de smartcard is, in tegenstelling tot de magneetstrip-kaart, niet kopieerbaar. Sleutels of passwords kunnen veilig in de kaart opgeslagen worden;
- de smartcard heeft een processor waarmee diverse taken uitgevoerd kunnen worden. Het is mogelijk om wederzijdse identificatie tussen de smartcard en een ander systeem te laten plaatsvinden. Daarnaast kan de smartcard de communicatie met andere systemen vercijferen waardoor afluisteren geen zin meer heeft;
- de smartcard kan multifunctioneel gebruikt worden. Hierdoor is het mogelijk verschillende (beveiligings)toepassingen op de smartcard te implementeren.

Het project Twobesmart

Het project Twobesmart (Toegangs- en WOrkstation BEveiliging met behulp van smartcards) heeft als opdracht om fysieke en logische toegangsverlening te implementeren met smartcards. Het onderzoek heeft zich toegespitst op het gebruik van één smartcard voor zowel de fysieke toegang tot ruimten, als de logische toegang tot werkstations. Het resultaat van het onderzoek is een prototype toegangsverleningssysteem.

Prototype

Het door de Twobesmart-projectgroep ontwikkelde prototype toegangsbeveiligingssysteem bestaat uit 4 zelfstandige onderdelen: smart- card, deurtoegang, PC-toegang en beheer (zie figuur).



smartcard

De smartcard is het centrale element van het systeem. Op de smartcard staan de autorisaties voor deur- en PC-toegang. Daarnaast bevat de smartcard een PIN-code en handtekeningkarakteristieken voor de identificatie van de gebruiker naar de smartcard toe. De gebruikte smartcard is een contactloze smartcard. De contactloze smartcard heeft als voordeel dat deze geen slijtage-gevoelige contacten heeft.

Deurtoegang

De deurtoegang is gerealiseerd met een aansluiting op het huidige in gebruik zijnde TOBIAS-toegangsverleningssysteem (TOegangsBewakend Informerend en Alarmerend Systeem) waarbij de magneetkaartlezer vervangen is door een smartcard-lezer en speciaal ontwikkelde software. Om toegang te verkrijgen moet een gebruiker de smartcard ± 0,5 seconde tegen de smartcard-lezer houden. In deze tijd wordt de TOBIAS-informatie van de smartcard gelezen en wordt bepaald of de gebruiker geautoriseerd is om de ruimte te betreden. Is dat het geval, dan wordt de deur geopend.

PC-toegang

Voordat een gebruiker met een PC kan werken moet hij de smartcard op de smartcard-lezer leggen. De smartcard controleert eerst of zijn eigenaar geautoriseerd is om op de betreffende PC te werken. Daarna wordt de identiteit van de gebruiker geverifieerd. Hiertoe wordt de persoon gevraagd om een PIN-code in te tikken of om een handtekening te zetten. Indien én de autorisatie én de identificatie kloppen kan de persoon op de PC gaan werken.

Als de gebruiker na een tijd even de werkplek wil verlaten en de PC niet onbeveiligd wil laten staan, pakt hij zijn smartcard van de lezer en loopt weg. De PC kan nu door niemand anders gebruikt worden. Het toetsenbord en de muis kunnen niet worden gebruikt en het scherm is zwart. Nadat de oorspronkelijke gebruiker bij terugkomst zijn smartcard weer op de lezer gelegd heeft kan er verder gewerkt worden.

Beheer

Het beheer bestaat uit drie onafhankelijke applicaties.

- Algemeen beheer. Dit beheerprogramma registreert en personaliseert de smartcards. Er wordt vastgelegd wie er een smartcard hebben. Daarnaast worden algemene persoonsgegevens te zamen met PIN-code en handtekeningkarakteristieken op de smartcard geschreven.

- Deurtoegangbeheer (SMARTSPAR). SPAR is het beheerprogramma dat gebruikt wordt om de TOBIAS-magneetstripkaarten te beschrijven. Dit beheerprogramma is aangepast tot SMARTSPAR om ook TOBIAS-informatie op smartcards te kunnen schrijven.

- PC-toegangbeheer. In PC-toegangbeheer worden de PC-autorisaties van de gebruikers geregistreerd, bewerkt en op de smartcard weggeschreven.

Veiligheid en multifunctionaliteit

Tijdens de ontwikkeling van het prototype hebben twee aspecten van de smartcard centraal gestaan: veiligheid en multifunctionaliteit. Deze twee aspecten zijn uitermate belangrijk bij acceptatie van smartcard-systemen door de gebruikers, naast normale aspecten als gebruikersvriendelijkheid.

Veiligheid

De smartcard heeft in eerste instantie alleen een beveiligd geheugen. Dit is echter niet voldoende om de smartcard veilig te gebruiken.

Daarom is er een aantal beveiligingselementen toegevoegd:

- een smartcard communiceert alleen met een ander systeem nadat ze elkaar wederzijds geïdentificeerd hebben;

- de communicatie wordt telkens met een nieuwe sleutel vercijferd;

- bepaalde gegevens zijn beveiligd met speciale sleutels. Alleen systemen die deze sleutel kennen kunnen deze gegevens lezen en veranderen;

- de smartcard blokkeert blijvend of tijdelijk indien er te vaak een foute PIN-code, handtekening of sleutel gegeven wordt.

Mulitifunctionaliteit

In het huidige systeem zijn maar twee functionaliteiten op de smartcard ondergebracht, maar het moet mogelijk zijn om in de toekomst functio-naliteiten toe te voegen, bijvoorbeeld voor gebruik als debet-kaart (koffiepas).

In de beschrijving van het beheer is deze modulariteit al duidelijk te zien. Het algemeen beheer regelt de zaken die niets met specifieke applicaties te maken hebben en voorziet de smartcard van gegevens en functies die alle applicaties kunnen gebruiken. Iedere applicatie die op de smartcard staat heeft een apart deelbeheer. De deelbeheren hebben ieder een met sleutels afgeschermde ruimte van de smartcard tot hun beschikking en kunnen niet bij elkaars gegevens komen.

smartcard-proef

Het hierboven beschreven prototype is een half jaar gebruikt in een pilot in het PTT-hoofdkantoor te Groningen. Bij de concernstaven Bedrijfsveiligheid en Informatiemanagement is een aantal PC's en deuren beveiligd met het prototype. Gedurende de proef heeft PTT Research gebruikersaspecten alsmede technische en organisatorische aspecten van het systeem geëvalueerd.

Eén van de gevonden knelpunten van multifunctionele smartcards is hetbeheer en de opzet van de organisatie waarin beheer moet plaatsvinden. Doordat er verschillende applicaties beheerd moeten worden neemt de complexiteit van het beheer toe. Daarom zijn Bedrijfsveiligheid en PTT Research gestart met het opzetten van een beheerstructuur waarin rekening gehouden wordt met de eisen van alle betrokken afdelingen met betrekking tot beheer.

Verder is uit de proef naar voren gekomen dat het bestaande TOBIAS-toegangsverleningssysteem eenvoudig is uit te breiden naar een veiliger systeem met behulp van smartcards. Daarbij hebben de gebruikers de voorkeur uitgesproken voor een handsfree te gebruiken systeem waarbij de smartcard op een grote afstand uitgelezen wordt. Het is dan niet meer nodig de smartcard in of bij een lezer te brengen. Overigens is de gebruikte smartcard in de proef als eenvoudig en gebruikersvriendelijk ervaren.

Ontwikkelingen

Naar aanleiding van de proef en evaluatie is Bedrijfsveiligheid in samenwerking met een groot aantal betrokken afdelingen gestart met een vervolgproef in het Hunzehuys te Groningen. In deze vervolgproef wordt het gebruik van smartcards in een operationele omgeving getest. In de proef wordt de smartcard in eerste instantie alleen gebruikt voor fysieke toegangsverlening. Gedurende de proef moeten andere functionaliteiten toegevoegd worden.

In de toekomst kan de smartcard de huidige in omloop zijnde magneetkaarten bij PTT (TOBIAS-pas, koffiepas) gaan vervangen. Tevens kan de smartcard gebruikt worden om andere, nieuwe functionaliteiten (telefoonkaart, etc.) op onder te brengen. Op deze manier kan de smartcard evolueren tot een multifunctionele medewerkerskaart, zodat uiteindelijk iedere PTT-medewerker slechts één kaart voor intern PTT-gebruik nodig heeft.

Samenvatting

De smartcard heeft door zijn specifieke eigenschappen goede mogelijkheden om de magneetkaart op den duur te vervangen. PTT Research heeft een prototype-toegangssysteem ontwikkeld waarbij de smartcard multifunctioneel gebruikt is. De uitbreiding van het TOBIAS-toegangsverleningssysteem met smartcards is succesvol gebleken en heeft inmiddels een vervolg in een nieuwe proef. Een belangrijk aandachtspunt is het beheer van multifunctionele smartcards en de organisatie waarin dit plaatsvindt. In de toekomst kan de smartcard dienst gaan doen als multifunctionele medewerkerskaart voor iedere PTT-medewerker.

Adressen PTT Research

Technisch-wetenschappelijk onderzoek

Dr Neher Laboratorium
St. Paulusstraat 4
Leidschendam
Postbus 421
2260 AK Leidschendam

Telefoon:(070) 332 56 02
Telefax: (070) 332 64 77
Memocom:
Mailbox 27:NPS 1353

Europaviljoen
Winschoterdiep OZ 46
Groningen
Postbus 15000
9700 CD Groningen

Telefoon:(050) 82 10 00
Telefax: (050) 12 24 15
Memocom:
Mailbox 27:NPS 1126

Sociaal-wetenschappelijk onderzoek

Duindoorn 31
Leidschendam
Postbus 421
2260 AK Leidschendam

Telefoon:(070) 332 35 95
Telefax: (070) 332 95 08

Stationsplein 7
Groningen
Postbus 15000
9700 CD Groningen

Telefoon:(050) 82 25 34
Telefax: (050) 82 29 80