Een chipkaart voor de RUG: hoe en waarom?

Hans Kun賴a href="mailto:a.j.kune@bureau.rug.nl">a.j.kune@bureau.rug.nl

In september 2001, zo is de bedoeling, zal binnen de RUG de eerste versie van de elektronische leeromgeving een feit zijn. Alle studenten en docenten van de RUG en een flink deel van de overige medewerkers zullen dan via Internet toegang tot die omgeving krijgen. Op die omgeving staan veel persoonsgebonden gegevens, waaronder ook gegevens die privacygevoelig zijn. Een student zal er bijvoorbeeld op kunnen opzoeken welke cursussen hij kan doen (persoonsgebonden) en wat voor cijfers hij gehaald heeft (persoonsgebonden en privacygevoelig).

Voor de elektronische leeromgeving is het dus erg belangrijk, dat goed vastgesteld kan worden, wie er probeert in te loggen en vervolgens wat die persoon op het netwerk allemaal mag doen en zien. De gebruikelijke username ? password beveiliging is voor een dergelijke omgeving niet meer betrouwbaar genoeg. En dus moet er iets beters verzonnen worden, een betere authenticatie en autorisatiemethode, zoals de deskundigen dan zeggen. En dan valt al snel het woord ?chipkaart?. Binnen de RUG wordt daarom gewerkt aan de vormgeving van een chipkaartproject, dat tot doel heeft de toegang tot het netwerk van de RUG goed te beveiligen. Zal het dan toch nog zover komen dat alle RUG-studenten en medewerkers een chipkaart krijgen? Er zijn mensen (en daaronder hele verstandige) die bij het woord ?chipkaart? de rillingen over de rug voelen lopen. Dat komt in de eerste plaats doordat chipkaartprojecten erg simpel klinken, maar in de praktijk complex blijken te zijn. Chipper en chipknip zijn voorbeelden van projecten die veel moeizamer zijn verlopen dan iedereen van te voren voorzag en het studentenchipkaart project dreigt zelfs een roemloze dood te sterven, nu de Stichting Studenten Chipkaart in surs顛ce van betaling is terecht gekomen. De vraag is dus: hoe kunnen we ervoor zorgen dat een chipkaart voor de beveiliging van het RUG-Intranet niet hetzelfde droeve lot deelt? Het antwoord op die vraag is: het gaat niet om de kaart, maar het gaat om de authenticatie. De deskundigen spreken daarom liever van een auhenticatie-service, dan van een chipkaart, waarbij ze in het achterhoofd hebben, dat de service wellicht ook wel met geheel andere middelen geleverd kan worden, dan met zo?n kaartje. In de toekomst dient zich wellicht de mogelijkheid aan door middel van vingerafdrukken vast te stellen wie er op het netwerk probeert in te loggen, of door middel van irisspectroscopie, of stemanalyse. En in het begin van het project is het wellicht beter niet gelijk met een chipkaart van start te gaan, maar met een eenvoudiger middel, zoals bijvoorbeeld een token, dat de gebruikers van OPRIT wel kennen. Het gaat met andere woorden meer om de infrastructuur, die

het mogelijk moet maken eenduidig vast te stellen wie er inlogt, dan om het zichtbare en tastbare materi묿 middel dat aan de gebruiker ter hand gesteld wordt. Dat laatste zou flexibel inwisselbaar moeten zijn, afhankelijk van de mogelijkheden die de technologische ontwikkelingen bieden. Desondanks wordt er binnen de wandelgangen van de RUG ? en in wijder verband: binnen SURF ? toch vaak over een nieuw chipkaartproject gepraat, omdat op dit ogenblik de chipkaart het meest handige en meest voor de hand liggende middel lijkt te zijn, waarmee de authenticatieproblematiek kan worden opgelost.

Authenticatieproblematiek

De authenticatieproblematiek kent twee aspecten. Het eerste aspect is, dat een beveiliging van een netwerk met alleen username en password in de door en door slechte en verdorven wereld waarin we moeten leven onvoldoende is geworden. De kans dat een goede combinatie geraden wordt door een hacker is te groot en de communicatie tussen de gebruiker en de server kan afgeluisterd worden. Met een extra materieel middel wordt het hackers een stuk moeilijker gemaakt. De gebruiker heeft dan iets en hij moet iets weten. Nogmaals: dat ?iets? dat een gebruiker heeft, hoeft geen chipkaart te zijn. Er zijn ook ringen in de handel, die een gebruiker om zijn ringvinger kan doen en die een code afgeeft aan een apparaatje. Er zijn sleutelhangertjes die hetzelfde doen, ballpoints en ga zo maar door. In principe doet dat er allemaal niet zo toe: de gebruiker heeft iets (een vinger, een oog of een kaartje), via 驮 of ander leesapparaatje wordt dat iets aan de authenticatieserver doorgegeven en vervolgens wordt de gebruiker

ook nog eens gevraagd een pincode of een wachtwoord in te voeren. Klopt de combinatie volgens de authenticatieserver, dan krijgt het netwerk, en wel de autorisatieserver, het bericht dat persoon X legaal ingelogd is en de autorisatieserver zorgt er dan voor dat de gebruiker op het net precies datgene mag doen, waar hij rechten voor heeft gekregen, niet minder en vooral niet meer. Of dat nu honderd procent veilig is? Nee, natuurlijk niet. Er kan nog van alles misgaan. Zelfs vingerafdrukken en stemprofielen schijnen vervalst te kunnen worden, en dingetjes als ringen, kaartjes en ballpoints kunnen uitgeleend worden door domme gebruikers, met pincode en al. Maar duidelijk is wel, dat het veiliger is dan alleen maar een username en password combinatie. Zeker wanneer bedacht wordt, dat het met de chipkaarten (en al die andere dingen) ook mogelijk is de communicatie tussen de gebruiker en de server te versleutelen. Het tweede aspect van de authenticatieproblematiek is, dat de infrastructuur helder en effici륶 moet zijn. Het moet zo zijn, dat de gebruiker 驴 kaartje heeft en 驴 wachtwoord, kortom 驴 account. Daarmee moet hij/zij overal aan de RUG en ook daarbuiten kunnen inloggen. Er moet met andere woorden 驴 centraal punt zijn, waar de controle op het inloggen plaatsvindt en 驴 database, waarin de toegekende rechten opgeslagen liggen. Op dit ogenblik is aan die voorwaarde binnen de RUG niet voldaan. Toegangscontroles voor medewerkers vinden op lokale netwerken plaats en daarnaast is er de toegangscontrole met behulp van een token voor OPRIT-gebruikers; er is geen centrale authenticatieservice. En de toedeling van gebruikersrechten is zo mogelijk nog verder gefragmentariseerd. De invoering van een chipkaart is tegen deze achtergrond in de eerste plaats een project dat eenheid in de fragmentatie schept: alle neuzen op alle faculteiten moeten dezelfde kant op gaan staan en alle verantwoordelijken moeten het eens worden over de manier waarop de centrale authenticatiedienst opgebouwd wordt en hoe de autorisatie technisch gezien geregeld wordt. Pas als dat voor elkaar is, is de basis gelegd voor de kaart zelf (of de dasspeld voor mijn part), met alle haken en ogen en logistieke problemen die daaraan vast zitten. Een chipkaartproject heet wel een chipkaartproject, maar is in de kern van de zaak een Authenticatie en Autorisatie Service Project.

SURF

Wanneer wij Centrale Authenticatie Service zeggen, kunnen wij ons natuurlijk afvragen: hoe centraal moet die dienst zijn? Duidelijk is dat het voor de RUG minimaal een universitaire dienst moet zijn, maar denkbaar is ook dat het een landelijke dienst is, die voor het gehele Hoger Onderwijs opgezet is of zelfs voor het gehele onderwijsveld. Daar zouden allemaal goede argumenten voor zijn: de schaalvergroting zou een forse daling van de kosten per chipkaart met zich meebrengen en -misschien nog wel belangrijker- studenten zouden met 驴 chipkaart toekunnen voor alle universiteiten en hogescholen waar ze in hun studieloopbaan mee te maken krijgen. Er zijn natuurlijk ook goede argumenten tegen een landelijke authenticatiedienst: het is altijd erg moeilijk om landelijke diensten op te zetten omdat de universiteiten en hogescholen nu eenmaal niet alleen samenwerken met elkaar, maar ook tegen elkaar concurreren. En zelfs waar wel samengewerkt wordt, kan er nog heel veel misgaan: de surs顫ce van betaling van Stichting Studenten Chipkaart is daar het bewijs van. Binnen de Stichting SURF worden de argumenten pro zwaarder gevonden dan de argumenten contra: de Stichting heeft een initiatief ontplooid om alle universiteiten en hogescholen achter een nieuwe chipkaart te krijgen, die in september 2001 ingevoerd zou moeten worden. De meeste universiteiten hebben voorzichtig positief gereageerd op dit initiatief en het ziet er inderdaad naar uit dat de oude Stichting Studenten Chipkaart door een nieuwe chipkaart stichting opgevolgd zal worden, die zich ongetwijfeld ook met een nieuwe naam zal gaan tooien om het verschil met de oude en grotendeels mislukte kaart goed aan te geven. Dat verschil zal overigens inderdaad fundamenteel zijn. De studentenchipkaart, zoals die aan enkele universiteiten ingevoerd is (ook heel kort aan de RUG), ging uit van de gedachte dat het goed zou zijn de kaart voor zoveel mogelijk functies te gebruiken. Studenten zouden ermee kunnen betalen, bijvoorbeeld, en het zou de afzonderlijke universiteiten vrijstaan er allerlei aanvullende gegevens op te zetten. De nieuwe stichting zal zich in afwijking daarvan louter en alleen op de authenticatie richten. Dat betekent dat de kaart vrijwel geen gegevens bevat. Het enige gegeven dat een kaart bevat is een nummer (dat voor iedere kaart uniek is). Bij de uitgifteprocedure zal een studentnummer of werknemernummer in de centrale authenticatie database aan dit kaartnummer gekoppeld worden en op basis daarvan kan een centrale landelijke authenticatieservice opgezet worden. De autorisatieservice blijft geheel de verantwoordelijkheid van de universiteiten en hogescholen zelf. Of dit landelijke scenario werkelijkheid wordt of niet, ligt nog in de schoot van de toekomst besloten. In september aanstaande zal er meer duidelijkheid zijn. Duidelijk is wel, dat de uitsluitende gerichtheid op die ene dienst: authenticatie het voor de afzonderlijke instellingen mogelijk maakt alvast hun eigen infrastructuur in orde te brengen. Zoals hierboven

gezegd: die infrastructuur technisch en organisatorisch opzetten is eigenlijk het belangrijkste werk. Heb je die eenmaal, dan maakt het niet zo vreselijk veel meer uit of je de authenticatieservice zelf op het RC verricht of uitbesteedt aan een landelijke stichting.

Chipkaart

Op dit ogenblik wordt er aan de RUG hard nagedacht over de vormgeving van een authenticatieproject, dat in de wandelgangen natuurlijk chipkaartproject heet. Naar alle waarschijnlijkheid zal het project in het najaar definitief opgericht worden. De belangrijkste opgave zal zijn: over de gehele universiteit heen een draagvlak scheppen, dat centrale authenticatie en goede autorisatie mogelijk maakt. Dat is geen makkelijke taak, maar onmogelijk is ze ook niet: de buurman van de RUG, het AZG, heeft een dergelijk project met succes afgerond. Laten we het er dus maar op houden, dat we voor het jaar 2001 een plekje voor een nieuwe kaart in onze portefeuille moeten reserveren. De RUG-chipkaart. Op uw betaalkaart na de belangrijkste kaart die u ooit gehad heeft. Want zonder die kaart zult u het RUG-netwerk niet meer op kunnen en als u dat niet kunt zult u niet meer kunnen werken of studeren en zeg nu zelf: wat is er belangrijker op deze wereld dan achter het beeldscherm arbeidzaam bezig te zijn?

Begin pagina

---

index Pictogram 4