Afstudeerplan Paul van Leeuwen (0445142)

Probleemstelling
Steeds meer mensen maken gebruik van internet om te handelen. Er zijn verschillende methoden om te betalen via internet. Twee daarvan zijn creditcards en iDeal. Creditcards zijn al bijna een eeuw oud, iDeal daarentegen is een relatief nieuw systeem. Beide kunnen ze in dezelfde context worden gebruikt. Uiteraard roept dit vragen op wat betreft de veiligheid van beide systemen. Het probleem dat onderzocht gaat worden is als volgt:

Wat zijn, bekeken vanuit het perspectief van de klant, de veiligheidsrisico's van betalingen verricht met het iDealsysteem vergeleken met betalingen verricht met een creditcard? Welke beveiligingsmaatregelen zijn per systeem nodig om bepaalde aanvallen tegen te kunnen houden? Het gaat uitsluitend om on-line betalingen en uitsluitend om betalingen binnen Nederland.

Van de veiligheidsrisico's zal een diepere analyse worden gemaakt.

Op dit moment is er nog geen vergelijkend overzicht van de veiligheidsrisico's van deze twee systemen. Bovendien is iDeal een vrij nieuw systeem waarover nog weinig bekend is.

De volgende zaken zullen voor beide systemen in kaart worden gebracht:

- Threats: welke aspecten van de systemen kunnen onderhevig zijn aan aanvallen?
- Aanvallen: welke aanvallen zijn mogelijk en op welke threats?
- Per aanval het risico dat zo'n aanval kan worden uitgevoerd en de impact van een geslaagde aanval.
- Scenario's: specifieke uitwerkingen van aanvallen.
- Wat heeft een hacker te winnen, ofwel wat zijn de voordelen die voor een hacker te behalen zijn die hij niet kan behalen zonder een aanval uit te voeren?
- Welke aanvallen kan een hacker uitvoeren om dit voordeel te behalen?
- Wat kan een gebruiker doen om veilig van de systemen gebruik te kunnen maken?

Werkwijze
de probleemstelling kan worden uitgewerkt in abstractielagen. De volgende abstractielagen zijn gespecificeerd:

Systemen	iDeal en creditcard
Security requirements	Confidentiality, data authentication, entity authentication, non-repudiation (uit Tanenbaum).
Threats	Security issues, gegroepeerd onder de bovenstaande deelgebieden
Aanvallen	Mogelijke aanvallen op de onder 'Threats' genoemde issues.
Scenario's	Specifieke scenario's om de aanvallen onder 'Aanvallen' daadwerkelijk uit te voeren.

Door het bestuderen van literatuur worden de veiligheidsrisico's onder 'Threats' in kaart gebracht, voor zover dat mogelijk is. Het gaat hier om theoretische risico's om een zo volledig mogelijk overzicht te krijgen.

Onder 'Aanvallen' komen theoretisch mogelijke aanvallen op de onder 'Threats' genoemde issues. De theoretische aanvallen worden opgezocht in de literatuur. Voorbeelden van theoretische aanvallen zijn de Replay Attack en de Man in the middle attack.

Onder 'Scenario's' worden specifieke scenario's uitgewerkt waarmee daadwerkelijk een aanval kan worden uitgevoerd. Een voorbeeld daarvan is: Trudy mailt een trojan naar Alice waardoor de webbrowser van Alice wordt gehacked. Deze trojan zorgt ervoor dat het verkeer naar de website van een bepaalde merchant wordt omgeleid via een server van Trudy. Dit is een voorbeeld van een Man in the middle attack om de confidentialiteit en integriteit van een specifieke order aan te vallen. Deze scenario's worden gecreëerd door toepassing van de literatuur over mogelijke aanvallen.

De risico's en impact van een bepaalde aanval worden zoveel mogelijk uit de literatuur gehaald.

Literatuur

[Tan2002]	Andrew S. Tanenbaum (2002) / Computer Networks / Prentice Hall PTR
[Claes2001]	On the Security of Today's On-line Electronic Banking Systems. (27-12-2001). Opgevraagd 2-1-2007 op http://joris.claessens.ws/pub/stoebs.pdf
[Schot2007]	Bart Schotten (2007) / Een Vergelijking van Elektronische Betaalmethoden voor E-commerce / Bachelor Thesis Radboud University Nijmegen

Planning

9/11/2007	Inleiding met uitleg over iDeal en credit card en de specificaties van de security requirements
19/11/2007	In kaart brengen van de noodzakelijke aannames en verankering
23/11/2007	Operationalisatie gereed voor zover de variabelen die geoperationaliseerd moeten worden bekend zijn. Bij de operationalisatie worden variabelen voorzien van een meetniveau zodat ze onderling kunnen worden vergeleken.
3/12/2007	Mogelijke voordelen voor hacker in kaart gebracht
13/12/2007	Threats kaart gebracht
25/1/2008	Aanvallen in kaart gebracht.
22/2/2008	Scenario's voor specifieke aanvallen uitgewerkt.
7/3/2008	Conclusie gereed
21/3/2008	Uitloop

Overige
Er is in principe één keer per week, op vrijdag om 13.30, een voortgangsgesprek met de begeleider, Erik Poll. In de tussentijd kan altijd emailcontact plaatsvinden.