

Websurfen met onbetrouwbare computers

François Kooman <fkooman@student.ru.nl>

10 december 2006

Dit stukje is een samenvatting van mijn bachelorscriptie “Websurfen met onbetrouwbare computers”

Als een computer gebruikt wordt om bijvoorbeeld te internetbankieren wordt er vanuit gegaan dat deze computer betrouwbaar is. Dat wil zeggen dat hij niet voorzien is van bijvoorbeeld virussen en/of spyware. Als dat wel het geval is wordt het bankieren onveilig.

Een aantal banken in Nederland die online bankieren aanbieden maken gebruik van een ‘cardreader’ die in combinatie met bankpas en pincode gebruikt kan worden om in te loggen op de pagina en transacties te ondertekenen. Het probleem hiermee is dat de ondertekening ‘blind’ is. Dat wil zeggen dat je niet precies weet wat je ondertekent. Je ziet in je browser wat je gaat ondertekenen, maar dat kan aangepast zijn (zonder dat je weet of dat echt is wat je transactie inhoudt).

Er zijn een aantal zaken waar je als ‘aanvaller’ of schrijver van spyware rekening mee moet houden. Als de gebruiker goed oplet zal hij in de gaten hebben dat er iets mis is zodra de verbinding met de bank niet via SSL verloopt (het slotje ontbreekt, of de adresbalk wordt niet geel). Door nu een vals SSL-certificaat te importeren in de browser kan er gewoon een SSL-verbinding opgebouwd worden naar een andere computer zonder dat het opvalt. Dit omleiden van de gebruiker naar de valse website kan door middel van het configureren van een proxyserver in de browser. Weinig mensen zullen deze instellingen bekijken en het zal daardoor niet zo snel opvallen. Deze proxyserver handelt gewoon netjes al het verkeer af zoals het hoort, behalve verzoeken aan de website van een bank. Deze worden omgeleid naar de valse server. Daar het geïmporteerde SSL-certificaat er voor zorgt dat de verbinding netjes via SSL verloopt zal het nooit opvallen (behalve als het certificaat grondig onderzocht wordt door middel van een controle van de MD5/SHA-hash).

De valse website zal er voor zorgen dat alle verzoeken van de besmette computer direct voor ’t grootste deel transparant worden doorgestuurd naar de bank, met eventueel een paar subtiele wijzigingen. In mijn scriptie heb ik alleen gekeken naar het ‘afluisteren’ van bankgegevens die voorbij komen, zoals rekeningnummers, saldo informatie, overzicht van betalingen, creditcardnummers, etc. Het aanpassen van betalingen zal iets meer moeite kosten.

Het ‘mooie’ is dat dit allemaal werkt als je alleen gebruikersrechten hebt op de computer van de persoon bij wie je het bankverkeer wilt onderscheppen en/of manipuleren. Je hoeft dus als doelwit niet eens als beheerder te werken.

De oplossing voor dit probleem kan gezocht worden in meer geavanceerde cardreaders. Deze kunnen bijvoorbeeld de betalingen weergeven op een display zodat je *echt* weet wat je ondertekent en niet alleen wat je browser zegt. Dit zal echter een flinke investering vereisen van banken (of klanten) voordat hier iets uit kan komen. Wat je zelf bijvoorbeeld kunt doen is een ‘Live-CD’ van een GNU/Linux distributie downloaden (of bestellen). Bijvoorbeeld Ubuntu¹ of Knoppix². Je hebt dan in principe meer zekerheid van een veilig systeem.

Mijn scriptie (en presentatie) zijn te vinden op <http://www.student.ru.nl/fkooman/>.

1. Ubuntu website: <http://www.ubuntu.com>
2. Knoppix website: <http://www.knoppix.org>