

Websurfen met onbetrouwbare computers

François Kooman

Radboud Universiteit Nijmegen

29 juni 2006

Inleiding

Situatie en problemen

Aanval

Oplossingen

Conclusie

Inleiding

Onderzoek naar veiligheid online bankieren op een computer
geïnfecteerd met spyware

Spyware

Spyware is

- ▶ vaak ongemerkt geïnstalleerde software
- ▶ meestal ongewenst
- ▶ soms via EULA van veelgebruikte software (WMP)
- ▶ in staat activiteiten van de gebruikers vast te leggen
- ▶ in staat de werking van een computer aan te passen
- ▶ aanwezig op veel computers

Spyware II

Spyware is een probleem omdat het

- ▶ de privacy van gebruikers wegneemt
- ▶ wachtwoorden, creditcardnummers en bankgegevens kan achterhalen
- ▶ de computer kan inzetten om andere computers aan te vallen

Internetbankieren

Bankzaken via internet afhandelen

- ▶ loopt via versleutelde verbinding (HTTPS, SSL)
- ▶ wordt “beveiligd” door challenge/response systeem (autorisatie/authenticatie)
- ▶ gaat uit van betrouwbare computers

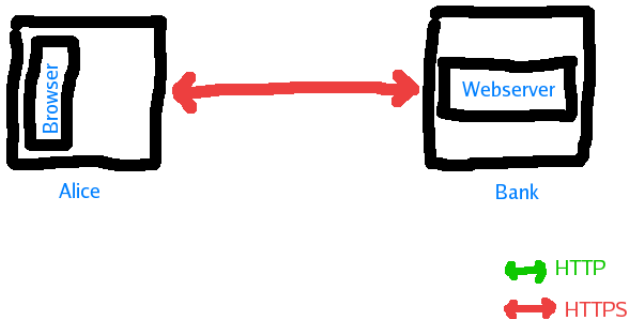
Is dit veilig als er spyware op de computer staat?

Situatie I

Internetbankieren werkt als volgt:

1. Gebruiker verzoekt webbrowser website te openen
2. Webbrowser maakt verbinding via HTTPS
3. Webserver stuurt een certificaat
4. Webbrowser controleert het certificaat
5. Webbrowser geeft de pagina weer

Situatie II



Problemen

Er kunnen problemen optreden als er spyware is geïnstalleerd bij

1. het maken van de verbinding met de server
2. het controleren van het certificaat

Aanval I

De verbinding kan “gekraakt” worden en het certificaatsysteem kan gefopt worden:

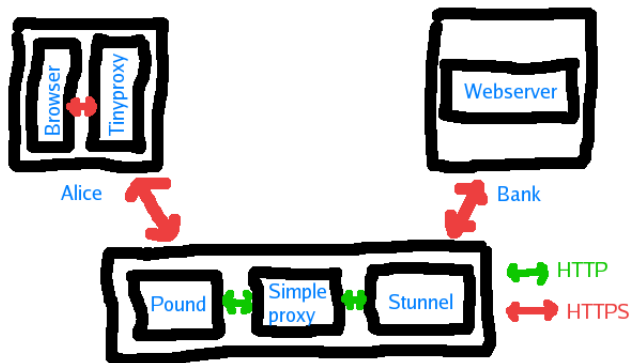
Omleiding

Omleiden verkeer door middel van een proxyserver op de computer van de gebruiker (MITM-proxy)

Valse certificaatautoriteit

Toevoegen valse certificaatautoriteit om te voorkomen adaat de webbrowser een waarschuwing geeft

Aanval II



Oplossingen

Oplossingen

De problemen zijn te minimaliseren of op te lossen door

- ▶ betrouwbare computers
 - ▶ besturingssysteem op read-only CD
 - ▶ “trusted” computing
- ▶ verificatie ondertekening van de transactie

Andere problemen

Het CA-systeem is eigenlijk ook onvoldoende (zelfs met betrouwbare computers)

Conclusie

Conclusie

Internetbankieren kan onveilig zijn op een computer met spyware

Demo

Kleine demonstratie als de tijd het toelaat. . .

Downloaden scriptie

<http://www.student.ru.nl/fkooman/>