Biometriese egtheidsbevestiging tydens intydse bankdienste

Authors:
Frans F. Blauw[1]
Sebastiaan H. von Solms[1]

Affiliations:
[1]Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa

Correspondence to:
Basie von Solms

Email:
basievs@uj.ac.za

Postal address:
PO Box 524, Aukland Park 2006, South Africa

How to cite this abstract:
Blauw, F.F. & Von Solms, S.H., 2013, 'Biometriese egtheidsbevestiging tydens intydse bankdienste', *Suid-Afrikaanse Tydskrif vir Natuurwetenskap en Tegnologie* 32(1), Art. #403, 2 page. http://dx.doi.org/10.4102/satnt.v32i1.403

Note:
This abstract was presented at the 'Studentesimposium in die Natuurwetenskappe 2011', presented under the protection of the *Suid-Afrikaanse Akademie vir Wetenskap en Kuns*. The symposium was held at the University of South Africa on 27–28 October 2011.

A system for biometric authentication in online banking. Online banking is under attack by cyber criminals using methods such as phishing, spoofing, and man-in-the-middle attacks. The system proposes using a biometrically secured USB stick containing the client's fingerprint, a unique key S, and a limited web browser and other information, which is provided to the client by the banking institution. To log on, the client allows his or her fingerprint to be read by the USB stick, and access is granted if the print matches the one previously stored on the USB stick. The browser on the USB stick is then activated, taking the client to the bank's real online banking web page. Every transaction is then secured by means of randomly generated session keys using the shared key S, the transaction information and other information. This system prevents many of the currently known malicious attacks.

Een van die doeleindes waarvoor die internet die meeste gebruik word, is vir finansiële transaksies, insluitende intydse bankdienste. Volgens 'n opname wat in 2009 gedoen is, maak 62% van bankkliënte van die intydse fasiliteit gebruik (Karim *et al.* 2009). Met die voordele kom egter ook nadele – indien 'n kliënt se intydse bankprofiel gekompromitteer word, kan dit groot verliese vir die kliënt beteken – sodanige profiele is die teiken van kubermisdadigers.

'n Intydse profiel kan volgens 'n verskeidenheid metodes gekompromitteer en aangeval word. Van die bekendste metodes sluit kuberstrikroof (*phishing*) (Irani *et al.* 2008), sleutelslag-aantekening (*key-logging*), spoefery (*spoofing*) en meer gesofistikeerde middelman-aanvalle (*man-in-the-middle attacks*) (Serpanos & Lipton 2001) in. Uiteraard is daar beskermingsmaatreëls ontwikkel om hierdie tipe aanvalle te voorkom, maar kubermisdadigers ontwikkel al meer gesofistikeerde nuwe aanvalsmetodes waarvoor dan weer nuwe beskermingsmaatreëls ontwikkel moet word.

Een van die bekendste beskermingsmaatreëls wat die meeste toegepas word, is om geldigheidsvasstelling (*authentication*) deur middel van die gebruik van eenmalige wagwoorde te doen. Wanneer 'n kliënt 'n sensitiewe finansiële transaksie deur middel van sy of haar intydse bankprofiel wil doen, byvoorbeeld 'n eenmalige betaling of die byvoeging van 'n nuwe begunstigde op sy of haar profiel, stuur die bank 'n gegenereerde wagwoord aan die kliënt se voorafgeregistreerde selfoonnommer. Hierdie wagwoord moet deur die kliënt ingetik word voordat die transaksie kan voortgaan. Die redenasie waarop dit gebaseer is, is dat slegs die werklike eienaar van die intydse bankprofiel toegang tot die betrokke selfoon het. (Die nommer word vooraf geregistreer wanneer die profiel aanvanklik by die bank geregistreer word.) Die proses bevestig dus die geldigheid van die eienaar. Desnieteenstaande is hierdie benadering vatbaar vir kuberstrikroof, spoefery en middelman-aanslae.

Hierdie navorsingsprojek stel 'n stelsel voor wat 'n intydse stelsel se vatbaarheid vir hierdie aanslae neutraliseer. Tydens aanvanklike registrasie ontvang die kliënt 'n biometries beskermde geheuestokkie (*USB stick*) van die bank. Die stokkie bevat 'n ingeboude vingerafdrukleser. Die kliënt se vingerafdruk sowel as ander inligting word dan op die geheuestokkie vasgelê. Die stokkie bevat ook 'n unieke sleutel, S, wat by die bank aan die kliënt se bankprofiel gekoppel word, asook 'n gemodifiseerde internetleser, wat direk met behulp van die geheuestokkie funksioneer.

Hierdie geheuestokkie funksioneer soos 'n doodgewone geheuestokkie, maar kan slegs geaktiveer en ontsluit word om met die kliënt se rekenaar te kommunikeer as die vingerafdruk wat aan die stokkie verskaf word en deur die stokkie gelees word, dieselfde is as die een wat aanvanklik tydens registrasie op die stokkie gestoor is. Die stokkie kan dus slegs deur middel van die oorspronklik geregistreerde eienaar se vingerafdruk geaktiveer word – dit verseker dus werklike geldigheidsvasstelling.

Wanneer die kliënt van sy intydse bankdiens gebruik wil maak, druk hy die stokkie in sy rekenaar in en ontsluit dit deur sy vingerafdruk te verskaf. As die stokkie suksesvol ontsluit is – wat slegs

deur die wettige eienaar (kliënt) gedoen kan word – gebruik sy of haar rekenaar die internetleser (*browser*) wat van die stokkie afgelaai word. Die leser se vermoë is baie beperk en kan slegs die bank se werklike, intydse bankdienswebbladsy bereik. Die kliënt is dus nou verseker dat die bank se werklike, korrekte bankdiensbladsy gebruik word, en nie 'n valse webbladsy nie.

Sodra die gebruiker sy of haar aantekenbesonderhede op die webbladsy insleutel, genereer die internetleser outomaties 'n eenmalige, tydsbepaalde wagwoord (TW) soos voorgeskryf in RFC 4226 (M'Raihi *et al*. 2005). Hierdie gegenereerde wagwoord, TW, maak gebruik van die wagwoord S, wat aanvanklik op die stokkie gestoor is en ook aan die bank bekend is. Die gegenereerde wagwoord TW word saam met die aantekenbesonderhede aan die bank gestuur, en die bank kan die geldigheid bepaal deur self S te gebruik om die eenmalige wagwoord TW te verifieer.

Voorts word elke verdere transaksie tydens die sessie op 'n soortgelyke manier beveilig. Die besonderhede van die transaksie word saam met die sleutel op die geheuestokkie S gebruik om 'n nuwe eenmalige wagwoord (NTW) te genereer. NTW is dus slegs geldig vir die transaksie waarvoor dit bereken is. Hierdie stelsel kan uitgebrei word deur die bank se identiteit-sertifikaat, gebaseer op publieke sleutelenkripsie, vir die asimmetriese enkripsie van die wagwoord te gebruik.

Die huidige implementasie kan op enige rekenaarstelsel werk, sonder die installering van addisionele programmatuur. Hierdie benadering sal die gebruiker tot voordeel strek deurdat sy of haar intydse bankprofiel teen kubersktrikroof, spoefery, middelman-aanslae asook die steel van aantekenbesonderhede beskerm sal word. Hierdie benadering sal verseker dat die transaksie wat versoek word, deur die werklike eienaar aangegaan word en nie deur 'n kubermisdadiger nie. Behoorlike geldigheidsvasstelling word dus afgedwing.

Literatuurverwysings

Irani, D., Webb, S., Giffin, J. & Pu, C., 2008, 'Evolutionary study of phishing', *eCrime Researchers Summit*, IEEE, 15 October 2008, pp. 1–10.

Karim, Z., Rezaul, KM. & Hossain, A., 2009, 'Towards secure information systems in online banking', *International Conference for Internet Technology and Secured Transactions*, Coll., London, November 9–12, pp. 1–6.

M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D. & Ranen, O., 2005, *HOTP: An HMAC-Based One-Time Password Algorithm*, besigtig vanaf http://www.ietf.org/rfc/rfc4226.txt

Serpanos, D.N. & Lipton, R.J., 2001, 'Defense against man-in-the-middle attack in client-server systems', *Proceedings of the IEEE Symposium on Computers and Communications*.

 doi:10.4102/satnt.v32i1.403