



Die modellering van potensiële persoonlike inligtingslekkasie deur die gebruik van sosiale netwerke

Author:

 C. Louw¹
Affiliation:
¹Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa

Correspondence to:

C. Louw

Email:

canlouw@gmail.com

Postal address:

PO Box 524, Auckland Park 2006, South Africa

How to cite this abstract:

 Louw, C., 2014, 'Die modellering van potensiële persoonlike inligtingslekkasie deur die gebruik van sosiale netwerke', *Suid-Afrikaanse Tydskrif vir Natuurwetenskap en Tegnologie* 33(1), Art. #1200, 1 page. <http://dx.doi.org/10.4102/satnt.v33i1.1200>
Note:

A selection of conference proceedings: Student Symposium in Science, 07 and 08 November 2013, University of Pretoria, South Africa. Organising committee: Mr Rudi W. Pretorius (Department of Geography, University of South Africa) and Ms Andrea Lombard (Department of Geography, University of South Africa), Dr Hertzog Bisset (South African Nuclear Energy Corporation [NECSA]) and Prof. Philip Crouse (Department of Chemical Engineering, University of Pretoria).

Modelling the potential leakage of personally identifiable information through online social networks. With the phenomenal growth of the online social network (OSN) industry, users have resorted to storing a vast amount of personal information on these sites. This information is not always adequately protected and can make its way, unintentionally, into the hands of individuals with malicious intent. We aim to model this process to the unsuspecting OSN user.

Weens die fenomenale groei en gebruik van sosiale netwerke (SN'e) stoor gebruikers al meer persoonlike inligting op sulke netwerke en op ander plekke in die kuberruimte. Te wyte aan gebruikers se onkundigheid oor die sekerheidsrisiko's wat inherent eie aan die Internet is, raak persoonlike inligting al meer die teiken van kubermisdadigers. Die aanvalle word vergemaklik deur gebruikers se swak sekerheidsinstellings op hulle slimfone en ander toestelle. Die onkundigheid en naïwiteit lei daartoe dat gebruikers persoonlike inligting op hulle SN'e stoor en dit met baie mense deel. Dit lei weer tot al meer lekkasies van persoonlike inligting.

Identiteitsdiefstal, kuberagtervolging (*cyber stalking*), afknouery deur 'kuberboelies' en vele ander onaangename gevolge vloe uit sodanige lekkasie van persoonlike inligting voort. Gebruikers van SN'e raak toenemend die slagoffers van sulke kuberaanvalle.

Die meer gesofistikeerde funksionaliteit van slimtoestelle, soos geoposisionering, waarby die toestel die presiese posisie van die gebruiker outomaties bepaal en saam met ander persoonlike inligting versend en stoor, vergroot net die risiko's vir die gebruiker.

Gebruikers sou aansienlik daarby kan baat as hulle die een of ander hulpmiddel kon verkry wat sou kan bepaal en aandui presies hoe die lekkasie van persoonlike inligting plaasvind en deur die sekerheidsinstellings van hulle slimtoestelle beïnvloed word. Indien 'n gebruiker fisies en visueel sou kan sien hoe sy of haar persoonlike inligting kan uitlek, sou bewustheid en die veiliger gebruik van SN'e bevorder word.

'n Stelsel wat visueel sou toon presies wie toegang het tot die persoonlike inligting wat gebruikers op hulle SN-profiel stoor, sou persoonlike inligting aansienlik beter beskerm. 'n Prototipe model wat juis dié funksie verrig, is tydens hierdie studie ontwikkel. Dit bied aan die gebruiker die volgende:

- die analisering van die gevolge van spesifieke inligtingstoegangsreëls wat verskillende gebruikers binne en buite die SN-struktuur moet gehoorsaam;
- die identifisering van kwesbare inligting op 'n SN-profiel;
- die identifisering van kwesbare inligting op 'n SN-profiel wat direk en indirek kan bydra tot die bepaling (afleiding) van verdere (private) inligting – ook bekend as inligtingslekkasie;
- eksperimentering met verskillende sekerheidsverstellings om inligtingslekkasies te verminder.

Hierdie prototipe model fokus op sewe kenmerkende stukke inligting wat op die meeste SN-profiel toeganklik is, en illustreer die proses van inligtingstoegang en lekkasie visueel. Hierdie illustrasie kan verbruikers 'n goeie aanduiding van moontlik kwesbare inligting op hul SN-profiel gee, en hulle in staat stel om aanpassings te doen waarvan die resultate dadelik sal blyk. Die einddoel van die prototipe is om gebruikers te help om te eksperimenteer om inligtingslekkasies op hulle SN-profiel te beheer.

Read online:


Scan this QR code with your smart phone or mobile device to read online.