International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:9, 2014

Protecting the Privacy and Trust of VIP Users on Social Network Sites

Nidal F. Shilbayeh, Sameh T. Khuffash, Mohammad H. Allymoun, Reem Al-Saidi

***Abstract*—**There is a real threat on the VIPs personal pages on the Social Network Sites (SNS). The real threats to these pages is violation of privacy and theft of identity through creating fake pages that exploit their names and pictures to attract the victims and spread of lies. In this paper, we propose a new secure architecture that improves the trusting and finds an effective solution to reduce fake pages and possibility of recognizing VIP pages on SNS. The proposed architecture works as a third party that is added to Facebook to provide the trust service to personal pages for VIPs. Through this mechanism, it works to ensure the real identity of the applicant through the electronic authentication of personal information by storing this information within content of their website. As a result, the significance of the proposed architecture is that it secures and provides trust to the VIPs personal pages. Furthermore, it can help to discover fake page, protect the privacy, reduce crimes of personality-theft, and increase the sense of trust and satisfaction by friends and admirers in interacting with SNS.

***Keywords*—**Social Network Sites, Online Social Network, Privacy, Trust, Security and Authentication.

I. Introduction

SOCIAL networking is a new way to communicate with users who can include all services tweets, blogs and posts. There are actually large numbers of artists and media organizations that take advantages of social networking, so that social media found a new type of conversation with existing customers, and also publish news and accept opinions. Social media is being employed to create a new type of conversation with existing customers, to gain new ones and to build credibility and reputation among expanding audiences. The social networking focuses on building communities and connecting like-minded people that share similar thoughts, hobbies and interests. The groups of users often have common interest called friends. They can exchange information including text, photos, graphics and videos with each other's quickly and easily.

A user's profile is generally what distinguishes social networking sites from other social media platforms such as owner sites or photo sharing sites. The profile helps setting the stage for building relationships with people who share the same activities, or personal contacts, to become a contact address with others. Through the user's profile, he can communicate with friends and publish ideas and information, exchange opinions, allow receiving requests from friendship and create groups on social networking.

Social Networking Site (SNS) is an Internet site that typically provides a core set of services in which members can build a personal profile, create and maintain a relational network of friends or contacts, and communicate with these individuals in various ways over the Internet [6], [9], [10]. Thus SNS allows members to create a personalized online community, which may or may not mirror offline connections. Specific SNSs, such as LinkedIn, Facebook™, and MySpace™, have developed reputations for catering to either particular types of members or for offering distinctive functionalities. For example, LinkedIn is often characterized as a SNS for professional contacts and makes available a method in which members can provide brief recommendations for others. Facebook™ and MySpace™ have developed reputations for having a large number of members who seek shared interests or educational backgrounds.

Privacy concerns in SNS are also attracting increasing public attention due to reports about privacy breaches on social networking sites [1], [3], [6], [12].

The increasing numbers of users of the social networking show that there are almost more than 400 million users, including what is provided by the SNS characteristics of successful activation like the establishment of social relations, friendships and participation in the information, where it has become a characteristic of modern times and their impact on political and social events, especially in the Middle East; What is called the Arab Spring (literally the Arabic rebellions or the Arab revolutions) is a revolutionary wave of demonstrations and protests that have been taking place in the Arab world since 18 December 2010. Arab Spring has proven its effectiveness as a hallmark of activation on the social networking and transfer of information, news, and comments without censorship and restrictions to the principle of activation of the freedom to the expression and the dissemination in social networks.

The social-networking success in communication and achieving all the goals that were specified for it, therefore, was associated with some threats that occur in a direct relationship with its success and the increasing number of users of who violate privacy for the purposes of entertainment or destruction. So the concern increased for the users vulnerable privacy violation, and the increased risks of dealing with social networking has become their opinion as an unknown region [15], [18].

Nidal F. Shilbayeh is with Computer Science Department, University of Tabuk, Tabuk 71491, Saudi Arabia, (phone: +966595978903; fax: +966 4 4223642; e-mail: nshilbayeh@ut.edu.sa).

Sameh T. Khuffash is with the Computer Science department, Al-Baha University, AL-Baha, Saudi Arabia, (e-mail: Sameh_khuffash@yahoo.com).

Mohammad H. Allymoun is with Computer Science Department, Middle East University, Amman, Jordan.

Reem Al-Saidi is with Computer Science Department, University of Jordan, Amman, Jordan.

However, SNS doesn't have the trust of all concepts including the trust of users in dealing with friends and favorite pages, because one can create accounts on social networking through a contract graphic with no official documentation proving the true character of such users, in addition to the mistrust in dealing seriously with most users who consider it as a network for entertainment and manipulation. Statistical studies have proven that some users tend to hide their real characters, so that they perform threats of the privacy and the credibility on social-networking, creating an environment that consists of fake representatives because they hide their real identities.

It has become an urgent need for VIPs and famous sites that have special accounts, on social networking (in order to communicate with fans and friends) to make their pages attractive and distinctive to reduce the threat of fake pages with negative effects on their reputation. There are some examples from the real threats and risks to the VIP.

II. Literature Survey and Related Works

Several new systems and architectures for privacy & trusted protection on social networking sites have been proposed**.**

The next generation social network to create a harmonious communication among its users using a multitude of service available on-demand any time, at a reasonable price based on usage, the idea is not only to develop a grail product but also to create an eco system around it to enable anyone who has an intent and content to carry out business [23].

Reference [24] proposes an architecture and implementation of a Social Cloud; an amalgamation of Cloud Computing, Volunteer Computing and Social networking. In their proposed system Facebook users can discover and trade storage services contributed by their friends, taking advantage of pre-existing trust relationships. In order to discourage free loading we have adopted a credit-based trading approach. Users may trade with a specific member of their Social network using a posted price market, or participate in an auction-based market. We have shown empirically that the marketplaces used for trading and/or reciprocation of services could be hosted using small scale resources, our system can perform multiple concurrent auctions that would satisfy the requirements for a moderately sized social.

A. Digital Signature Standard (DSS)

This Standard specifies a suite of algorithms that can be used to generate a digital signature. Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation, since the signatory cannot easily repudiate the signature at a later time.

A digital signature is an electronic analogue of a written signature; the digital signature can be used to provide assurance that the claimed signatory signed the information. In addition, a digital signature may be used to detect whether or not the information was modified after it was signed (i.e., to detect the integrity of the signed data). These assurances may be obtained whether the data was received in a transmission or retrieved from storage. A properly implemented digital signature algorithm that meets the requirements of this Standard can provide these services.

A digital signature algorithm includes signature generation process and signature verification process. A signatory uses the generation process to generate a digital signature on data; a verifier uses the verification process to verify the authenticity of the signature. Each signatory has a public and private key and is the owner of that key pair. the private key is used in the signature generation process. The key pair owner is the only entity that is authorized to use the private key to generate digital signatures. In order to prevent other entities from claiming to be the key pair owner and using the private key to generate fraudulent signatures, prior to the generation of a digital signature, a message digest shall be generated on the information to be signed using an appropriate approved hash function. Depending on the digital signature algorithm to be used, additional information shall be obtained. For example, a random per-message secret number shall be obtained for DSA. Using the selected digital signature algorithm, the signature private key, the message digest, and any other information required by the digital signature process, a digital signature shall be generated in accordance with this Standard.

B. FaceCloak: An Architecture for User Privacy on SNS

Reference [21] provided an architecture that protects user privacy on a social networking site by shielding a user's personal information from the site and from other users that were not explicitly authorized by the user. At the same time, FaceCloak seamlessly maintains usability of the site's services. FaceCloak achieves these goals by providing fake information to the social networking site and by storing sensitive information in an encrypted form on a separate server. We implemented our solution as a Firefox browser extension for the Facebook platform. The experiments show that solution successfully conceals a user's personal information, while allowing the user and his friends to explore Facebook pages and services as usual.

C. Privacy Protection for Social Networking Platforms

The privacy risks associated with social networking APIs by presenting a privacy-by-proxy design for a privacy-preserving API. Their design is motivated by an analysis of the data needs and uses of Facebook applications [7], [8], [16]. They studied 150 popular Facebook applications and found that nearly all applications could maintain their functionality using a limited interface that only provides access to an anonymized social graph and placeholders for user data. Privacy-by-proxy can be accomplished by using new tags and data transformations without major changes to either the platform architecture or application.

D. Protecting Users from Malicious Facebook Application

A user can legitimately assume that a social network provider adheres to strict privacy standards; we argue that it is

unwise to trust third-party applications on these platforms in the same way. Existing mechanisms are not convincing. Therefore, we introduce PoX, an extension for Facebook that makes all requests for private data explicit to the user and allows her to exert fine-grained access control over what profile data can be accessed by individual applications. By leveraging a client-side proxy that executes in the user's web browser, data requests can be relayed to Facebook without forcing the user to trust additional third parties, we consider PoX to be a readily available alternative for privacy-aware users that do not want to wait for privacy-relevant improvements to be implemented by Facebook itself [13].

E. A Collaborative Framework for Privacy Protection

The problem of data privacy has attracted much attention. Several approaches have been proposed to address this issue. One of privacy management approaches for OSN leverages a key management technique to enable a user to simply post encrypted contents so that only users who can satisfy the associate security policy can derive the key to access the data. However the key management policies of existing schemes may grant access to unauthorized users and cannot efficiently determine authorized users. They proposed a collaborative framework which enforces access control for OSN through an innovative key management focused on communities. This framework introduces a community key management based on a new group-oriented convergence cryptosystem, as well as provides efficient privacy preservation needed in a private OSN [22].

F. Privacy Wizards for Social Networking Sites

Privacy is an important emerging problem in online social networks. While sites such as facebook allow users fine-grained control over who can see their profiles, it is difficult for average users to specify this kind of detailed policy.

Reference [2] proposes a template for the design of a privacy wizard, which removes much of the burden from individual users. At a high level, the wizard solicits a limited amount of input from the user. Using this input, and other information already visible to the user, the wizard infers a privacy-preference model describing the user's personal privacy preferences. This model, then, is used to automatically configure the user's detailed privacy settings. To illustrate this idea in concrete terms, we have built a sample wizard, which is based on an active learning paradigm. We have also constructed a visualization tool, which allows advanced users to view and modify the resulting model. Our experimental evaluation, which is based on detailed privacy preference information collected from 45 Facebook users, indicates that the wizard is quite effective in reducing the amount of user effort, while still producing high-accuracy settings. The results also indicate that the community structure of a user's social network is a valuable resource when modeling the user's privacy preferences.

III. The Proposed Architecture

In this paper, we propose a new design of the FaceTrust architecture that gives trust and privacy to the Social Networking Site. FaceTrust will be applied on Facebook's platform because of the ease of evaluating, modifying settings of the content pages and the features in Facebook which allows adding a third party. It is simply a third party added on the social networking to increase the trust between users, especially VIPs, who are exposed to threat and risk when using social networking by reincarnation of personalities and fraud to spread lies on the Facebook pages.

FaceTrust and Facebook together achieve the objectives of protection for VIP users, to increase the performance and haste the completion of operations.

The design of FaceTrust is based on several principles:

- No specific browser performs the task: From the important properties dealing with designing, it is possible not to use a specific browser to apply Facetrust, so that it uses any type of the existing browsers and performs the functions automatically and a few interaction users tend to complete the procedures. Therefore, no changes to the browser's structure order except the design, the architecture automatically applies a Trust logo that appears on the profile page.
- No change in the architecture Facebook: The providers of SNS are interested in the financial cost; hence, achieving fundamental principles of social networking, in addition to the protection of privacy and trust for the VIPs to expose the threats did not take part in the interest of the social-networking providers. Generally there is no incentive for these providers to introduce changes to their system architecture for privacy protection, unless those changes have the financial gain or are legally required [21]. It thus can be applied to protect the privacy and the trust for the VIPs existence of a mechanism depends on the cooperation with a third party without changing the server side.
- Self-dealing and Minimal Interaction of users**:** The VIP users of social networks differ in technical skills, so that the levels ranging from high to weak according to the experience, in addition to make a privacy and trust protection as a solution suitable for all users regardless of their skills. Consequently, the solution should be self-dealing rather than depending on users to install additional software. For that reason, it requires minimal configuration in order to implement FaceTrust as a third party, that involves the VIPs users without having to download extra software, and thus the VIPs users follow a number of procedures to authenticate information by their own URL.
- FaceTrust Logo: The participation of VIPs in FaceTrust and the completion of procedures for electronic authentication and verification are important. In order to activate the account the trust logo should appear in the image of the profile page. The trust logo will be distinctive and unique which is not to copy and modify

illegally. Therefore, following the rules of security and protection on the logo increases the VIP's trust.

A. FaceTrust Architecture

To visit the link application, they must go to the application through Facebook. The VIPs enter their URL of their website, therefore, they will provide two parameters to Facebook, the URL & secret session, so that the personal information of the VIP is documented through the URL to make sure that the website is valid and to get the account information through the Facebook server. The account information is required to complete the registration process and to establish an account on FaceTrust, finally the information is stored in the database.

The next phase is the key creation, by using the encryption algorithm (SHA-1& hash function) through inserting (ID and activation link) to the algorithm. The result of the process is a password sent to the VIP's e-mails, so that it receives the email address in the content of the URL, in order to confirm the arrival of the service to the owner of the website .

Finally, the verification process of the identity of the applicant and make sure that the activation link is displayed, then click on the link to activate the trust logo on the profile picture.

Fig. 1 shows the main parts of the proposed architecture.

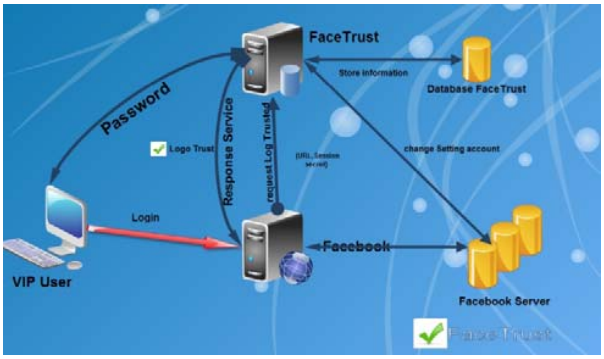


Fig. 1 FaceTrust Architecture

The main parts of FaceTrust Architecture: Social Networking & VIPs Users and FaceTrust.

B. Social Networking & VIP's Users

The VIPs can benefit from the service FaceTrust and the famous people, for example, artists, politicians, governmentals, writers, news sites, television sites and popular politician sites. You just need a specific website documented with information-related to the VIP, to make the pages on social networking distinctive and unique and so that the fan's inference on a page by FaceTrust logo can be seen on the image, as shown in Fig. 2. Therefore, the growing need to find a mechanism which can verify social-networking pages, especially the pages of the VIPs, in order to reduce the crimes of spoofing and exploitation of the VIP names illegally.

Fig. 2 Who is trusted?

The vandals following the method's social attack, because it's easy to create an account on the principle of trust, so without making sure of the users motivation so that the bad people exploits the VIPs names to publish news and information to convince fans that this is a VIP page, in addition to publishing lies and rumors to VIPs discredit. Moreover, it increases the number of fake pages that leads to increase the concern of fans.

The existence of the FaceTrust of application in a social networking environment and the Trust logo distinctive credibility to the VIP page, in order to give satisfaction to the fans and VIPs, in addition to ease the FaceTrust procedures that use electronic authentication, which is based on the information recorder on the VIPs website without following complicated procedures to authentication.

Each website contains information about the owner such as (site, name, address, email, phone number) which are documented and formally registered by the web hosting.

FaceTrust is applied on Facebook to raise the level of trust and to protect privacy, in order to reduce the threats and problems of related VIP pages. The FaceTrust is considered one of the most important effective methods to authenticate VIP pages on Facebook and easily identified by the Trust logo, therefore, allowing participants in logo FaceTrust by following simple procedures.

However, the FaceTrust and its relationship with the Facebook's network platform besides dealing as a cooperative third party and allows access to the VIP information with the capability to modify the page settings, so that the partnership between SNS and third-party applications is limited, especially when it comes to using and dealing with sensitive personal data, it is impossible for social networks to impose further constraints to use this data by the application, so they lack the means of protecting of privacy this data. The Facebook needs every application developer to accept the Terms Of Service (TOS) in order to get the approval of dealing with data; So these terms state that an application must not store collected data and be exploited illegally, in addition to the service to report the abuse and Facebook's ability to suspend the service, whether the third party increases complaints and violates terms.

C. FaceTrust

FaceTrust carries out privacy protection and gives trust in three processes: the configuration process, the registration process and activation & verification process. Fig. 3 shows the three processes.

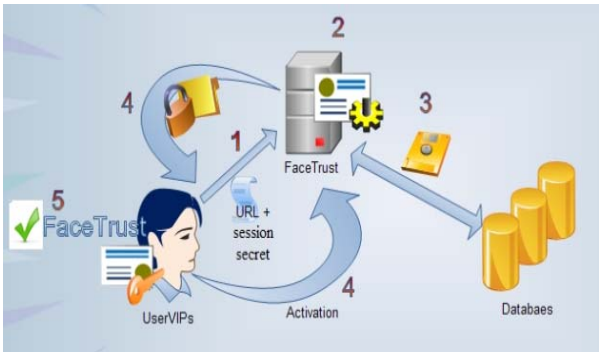


Fig. 3 The main processes of the FaceTrust architecture

The VIPs begin to get the trust service on the configuration process; in addition to the previous knowledge of users that FaceTrust is a third party on the Facebook and users should accept terms of service (TOS). In terms of FaceTrust application, the communication between the third party and Facebook is done by using the method of calling through the hypertext transfer protocol like GET or POST requests. The GET request: retrieves information from FaceTrust or Facebook profiles, and the POST request: adds information to an existing profile page and database. This means that FaceTrust applications can retrieve information from the VIPs profiles and post data on the database.

The first step, the users sign in the account of Facebook, they must visit the FaceTrust page via a link or clicking on the icon, hence a welcome screen appears explaining the service definition procedures and instructions to get the service, then to subscribe with FaceTrust. Moreover, to request the application requires permission to access personal information and the ability to modify the page settings, besides explaining the contract conditions to create the safe and reliable environment in Facebook. After that it accepts the VIPs on the permission request.

After the welcome screen is completed, and the agreement of the permission request, the FaceTrust asks the VIPs to enter the address of their website, accordingly the URL will be sent to the registration process, thus the configuration process is implemented.

The registrations process begins; the registration process will receive two values (URL and secret session) from the configuration process, then the URL in order to get information related to the identity stored within the content of the website that is already documented in the webhosting. Some examples of the contents of the URL are the following: (name, address, email, IP address, phone number). In addition to the reason of using a secret session in FaceTrust application is the ability to access information stored in the profile page without recognizing the user [17].

To ensure that FaceTrust applies in the Facebook platforms easily and effectively, the application is provided through the libraries to third-party developers, those libraries contain a set of different programming languages such as PHP, Python, java, C# or any web programming tool, in order to lead several functions to achieve the objectives effectively. For example, the registration process needs to get the VIPs information, so it calls the programming languages library to complete this process.

The communication that happens between FaceTrust application and Facebook servers is through social channels, by establishing channels automatically together in order to control the transfer of information.

The process of electronic authentication happens in the registration process to get information from the VIP's URL, the feature application which retrieves all the information contained within the URL [4], [11], [20]. It also stores the information in the FaceTrust database, as well, so that using the secret session to gather the personal information within the account of Facebook. As the registration process is completed the ID and activation link are sent in order to get a trust logo, and the activation & verification process is stored, as well.

Finally, the completion of the activation & verification process allows the trust logo to appear on the image profile and change the settings of pages, and display FaceTrust icon, accordingly leads to more trust and verification of the real identity. Moreover, it reduces the risk of fake pages. Fig. 4 shows the main processes of the FaceTrust.

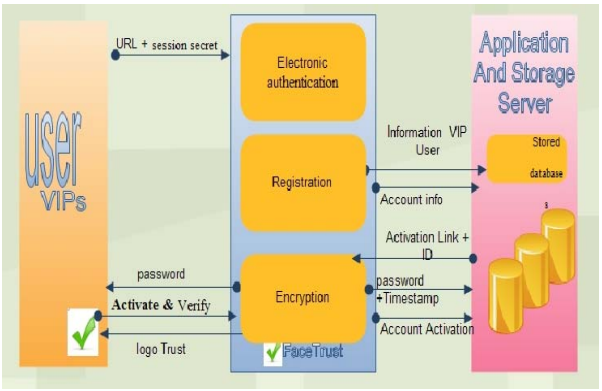


Fig. 4 The Main Processes FaceTrust

1. Configuration Process

The Configuration process is the first step in the FaceTrust architecture, it is selected through which the application of FaceTrust as a third party has been documented, and shared with Facebook after accepting restriction agreement (TOS) , as a result a special identifier (ID) ensues, implying communication with Facebook and compliance for the contract's conditions and terms.

The FaceTrust can use the Facebook Query Language (FQL), which is similar to Structured Query Language (SQL). The query languages are programming languages designed to retrieve, for example, information from databases and the Facebook server. In addition, FaceTrust can get information

about the VIP's user just by subscribing in the service, that's really what FaceTrust applications do to gather information and authentication about VIPs. FaceTrust could use this service as a way to create a trusted environment for VIPs or build real relationships with fans.

The configuration process does not need to load additional software or other applications, so that it does not have any extra burden or complicated procedures on the VIP's user, thus the following simple steps based on a series of screens, these screens are called OAuth dialog to explaining services in a form illustration. The user can handle the service no matter what the level of skills, experience and information technology. Might be only the ability to use Facebook and internet is enough.

The following steps are used in the configuration processes:

Step 1. Click on the icon of FaceTrust that appears on the Facebook page, or visit the application link after logging in the personnel account.

Step 2. The welcome screen appears on Facebook explaining the instructions and services of FaceTrust as well as privacy protection to give trust to VIPs.

Step 3. The permission request screen appears asking the user permission to access personal information, moreover, determine the privacy options that allow access through FaceTrust.

Step 4. Enter the URL on the FaceTrust screen, the VIPs set the address of their website, accordingly the URL is the website's address of the VIPs and it must be a website on the network.

The two values are (URL & secret session) are sent from the configuration process to the registration process.

2. Registrations Process

The registration process is the basic phase in FaceTrust in which several procedures are applied concurrently to complete the process to complete the trust logo process on the VIPs page.

It consists of several components; each component performs a particular function with FaceTrust; In addition, the operations to complete the trust and privacy protection process, as well as handling all the components in the registration process as a cooperative and integrated performance, comply with the different libraries of programming languages used in each component. All communications that happen between the components and FaceTrust are encapsulated by this library, thereby increasing the simplicity of work and cooperation if a third party has been added, in addition to the fact that performance increases and find the solutions to reduce the architecture of social networking problems, so that the problems will not arise according to increase the importance of the users of social networking.

Fig. 5 shows a parts of the registration process, which is composed of four components: Electronic Authentication, Registration Information, Stored Databases, and Encryption.

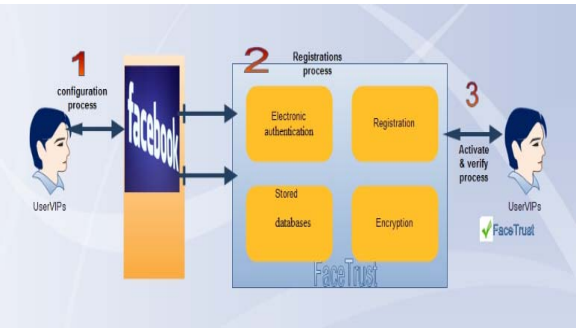


Fig. 5 Parts of the Registration Process

a) Electronic Authentication

The electronic authentication is a quality addition on the social networks and an effective mechanism to verify the identity of users as well as to know social-networking pages for VIPs, in order to reduce the risk of privacy threats, and the threats faced to the VIPs on social networking. Moreover the social networking is necessary and important to find an interactive environment between the fans.

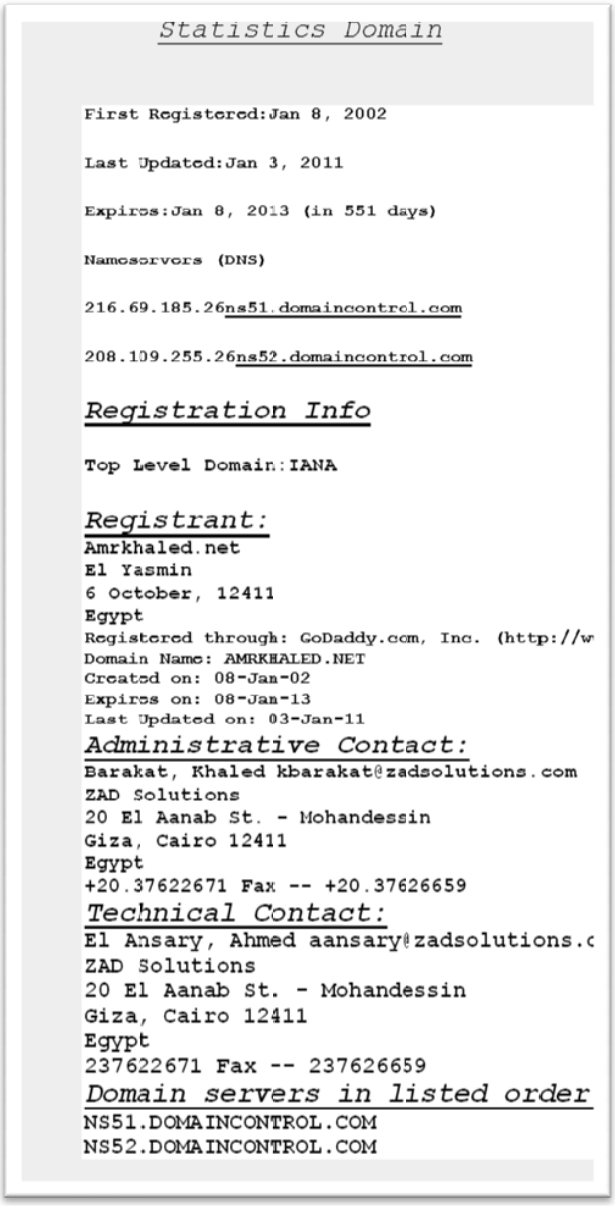
Electronic authentication is a mechanism for data collection and to get personal information with the authentication, so that it is easy to be used and handled by the application. Also, it is a smart way to find an effective method to verify the profile on social networking. Moreover, the procedures are free from complexities and thus finding the alternative solution rather than using paper documentation, in order to verify the person's identity by complicated paper transactions. Hence, the difficulty of applying verification on the user's identity, and VIP's unwillingness to commit to complex and restricted procedures to privacy, so using the electronic authentication is the most appropriate.

Therefore, to create an effective solution to achieve objectives of trust and privacy protection that meets the ambitions of the VIP at the same time. So, the idea of electronic authentication is documentation from something already recorded on the internet, which is documented by the website to operate based on documentation of personal information for applicant service. Also contact information such as (name, address, email, IP address web sites, phone number) must be documented data and stored in the webhosting; hence the idea of documenting data that are already registered will lead to the appearance of the trust logo, but just for the VIPs who have their own web site.

The registration process takes the URL from the configuration process, and uses the software and library programming languages to extract the VIP's information. FaceTrust application verifies the website address, and makes sure of its effectiveness, thus it has been avoiding the use of paper solutions to check the identity of users. Consequently, creating a technical solution uses the information documented in the URL, to get the information contained within the URL, WHOIS registration is used. WHOIS is a TCP-based transaction-oriented query/response protocol that can be used to provide information services to internet users, so that they are used to get the contents of the URL in order to be an

effective service to authenticate information about the website owner, besides, to benefit from verification and documentation of the category of users on the website. Then WHOIS protocol is used within the components of FaceTrust to get information of the website owner.

Fig. 6 shows how to extract information from the content of the URL by the WHOIS, this content of the site is of Dr. Amr Khaled (www.amrkhaled.net) using the WHOIS, in addition to finding domain names that show details of the personal information that can be obtained through the URL [11].



Statistics Domain

First Registered:Jan 8, 2002

Last Updated:Jan 3, 2011

Expires:Jan 8, 2013 (in 551 days)

Nameservers (DNS)

216.69.185.26ns51.domaincontrol.com

208.109.255.26ns52.domaincontrol.com

Registration Info

Top Level Domain:IANA

Registrant:
Amrkhaled.net
El Yasmin
6 October, 12411
Egypt
Registered through: GoDaddy.com, Inc. (http://w
Domain Name: AMRKHALED.NET
Created on: 08-Jan-02
Expires on: 08-Jan-13
Last Updated on: 03-Jan-11

Administrative Contact:
Barakat, Khaled kbarakat@zadsolutions.com
ZAD Solutions
20 El Aanab St. - Mohandessin
Giza, Cairo 12411
Egypt
+20.37622671 Fax -- +20.37626659

Technical Contact:
El Ansary, Ahmed aansary@zadsolutions.c
ZAD Solutions
20 El Aanab St. - Mohandessin
Giza, Cairo 12411
Egypt
237622671 Fax -- 237626659

Domain servers in listed order
NS51.DOMAINCONTROL.COM
NS52.DOMAINCONTROL.COM

Fig. 6 Extracted information from Amr Khaled URL contents

b) Registration Information

After completing the electronic authentication process successfully and making sure of the validity of information and the website, then setting a special form with information that contains all the details of those who seek the FaceTrust service, but also the information extracted from electronic authentication lacks of what is needed to fill all information in order to complete the process of registering subscribers, in addition to that, the lack of taking information is not available in the URL. Moreover, to obtain the missing information in the URL is through the personal information in the Facebook profile via using the secret session. Accordingly to take the image of VIPs will put the trust logo through the use of programming languages library to perform the task.

Fig. 7 shows the information form that requires filling in the information that is necessary to document the personal information; furthermore the FaceTrust depends on two ways to bring information:

1) The information extracted within the URL.
2) Information and image in the Facebook account through the secret session.

After finishing from the registration process, the activation link appears, therefore, FaceTrust sends this link to the VIPs after investigating the conditions of participation with it, thus when clicking on the link, it changes automatically all the settings of the page, hence, the trust logo appears on the personal image profile, and shows the icon of the FaceTrust on the Facbook menu bar so as to make modifications, revoke the service and enable to change some privacy.

c) Stored Databases

The storage process in the database is separated from Facebook which is important in order to work independently to protect trust and privacy for VIPs, without the intervention or control of Facebook, so that data is stored in the FaceTrust server in order to ensure the confidentiality and protection of information.

Accordingly, the collected information and the activation link are stored, which produces the registration component. Therefore, it is considered as a critical link for the implementation of the FaceTrust service and it gives trust to the Facebook profile, in addition to give the subscriber a new number, ID to deal with FaceTrust. Further, to follow several technical conditions that prevent the wrong exploitation to protect privacy and trust, as well as putting some restrictions on the stored information to ensure the provision of distinctive services and reduce the risk of violation. Also the threat against the social-networking sites appears so that the values are received from the configuration to be registered and stored.

Fig. 7 Important information necessary for the registration phase

It contains a database on a special field to activate the Facebook service in the activation & verification process. Moreover, to complete the signup, and the ability to change and modify the database information by the application at any time, thus to give the authority to enable the user to control the privacy of information.

The database contains fields to store an activation link and a field to store the password that comes from the encryption component, and also the field that contains a time counter, which is set in the time stamp to limit the time completing of the process of activating, and ensure that wrong exploitation. Consequently, the countdown starts from the moment of sending the link to the moment of activation time, to check if it exceeds the time required to cancel the account permanently from the database. Accordingly, confirm the access of the service to applicants, and minimize the service off for VIPs beneficiaries.

However, the operations are in the database that provides the usage of the server-side through Facebook Query Language (FQL), and retrieve information from the database MySQL in FaceTrust and scripts to simplify the task.

d) Encryption

The encryption component is used effectively on FaceTrust to ensure the security and protection of the transmitted information from FaceTrust to VIPs. In addition to considering that encryption is the conversion of activation links into a form called "a password" that cannot be easily understood by unauthorized user. It also works to manufacture the trust logo to be put inside the image, so manufacturing such logo by using the technical watermarking to distinguish this image.

- Generating Password

The password is one of the essential requirements that must be available in the architecture [14], which provides the required protection for VIPs to access the trust service, and makes sure that the identity is true, to increase the security and trust when dealing with users. Accordingly, we should resort to the technical methods to protect the activation link and confirm the service arrival to applicants by following several steps:

Step 1. Protection of the activation links that are sent from the FaceTrust to VIPs.

Step 2. Verification of the arrival of the activation link to the service seekers.

Step 3. Generating the password and send to VIPs so that it completes the registration process.

That is not the same encryption process as in messages or texts, thus this is a process of generating keys as a password, in order to be sent to VIPs through the e-mail, to be used later to activate the service with the appearance of the activation link and complete the registration process successfully.

Fig. 8 shows how to process the key generator, and it receives parameters (ID & activation link) from the database. Therefore, to use One-Way Hash functions, and also using many encryption algorithms such as SHA-1, a hash function is an algorithm that takes an (ID & activation link) as input, and produces a password as output [19]. Consequently, produce the text string that is computed by hash and display the result as the hex encoding, the result of the algorithm SHA-1 is called hashed password. Fig. 9 shows hashed password, accordingly, passwords that are stored from hashed in the FaceTrust database, and then sent to VIPs by the email which is located in the URL content. The time counter performs in a specific mechanism to ensure the verification and make sure of the access of service, as it must be activated during a specific time that limits should not exceed that time.

- Trust Logo Process

This part is for processing images to show the trust logo, so that the processing of an image is performed by using the watermarking technique and the FaceTrust logo to appear as a special mark within the image. After studying the solutions and graphics proposed for the trust logo, it attracts the attention of the friends and fans easily and without problems. It was agreed on the form of the trust logo that consists of the name of the FaceTrust and ID number as a predefined mark within the image by using a watermarking technique. Accordingly it is applied using the hidden watermarking techniques proposed and implemented by the first author in [25]. Adobe Photoshop is used to add the visible trusted watermark logo. Fig. 10 shows the process of producing trust logo.

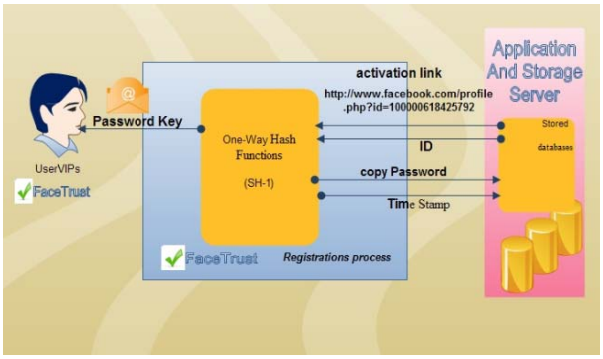


Fig. 8 Process Generator Key

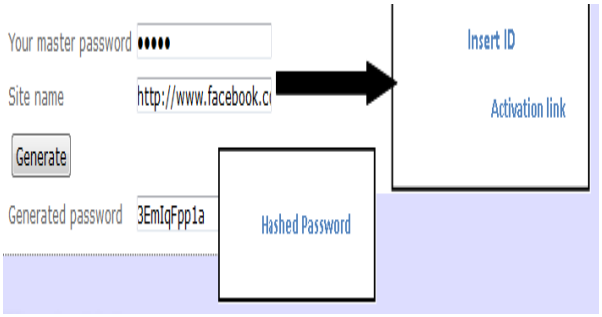


Fig. 9 Hashed Password by SHA-1

Fig. 10 Adding the trusted logo to the Image processing

The watermark effect is achieved by using Photoshop, thus creating a layer of colored text over the middle of the image, besides the setting its blend mode to “overlay” and reducing the darkness of the text layer to 60%. This creates a nice subtle effect and puts FaceTrust text into the layer, in addition to putting the ID number of the page owner, so it is possible for anyone who likes to join the page and infer from the image that includes a logo.

Otherwise the watermarking technique is used to produce the trust logo that appears in the image [5], thus finds a distinctive logo. It is easy to recognize users, through this mechanism is not to achieve protection of the image and prevent theft. So it is in no way able to protect the image by stealing logo and use it illegally.

- Activation & Verification

It is the final process in the FaceTrust application, thus the VIPs activate the trust service, and then the trust logo appears after completing the registration process. Consequently, to be on the FaceTrust, it verifies the identity of the applicant of the service, through several technologies that have been developed and used in the application to meet the criteria for security and the privacy protection. Additionally it gives trust for the social-networking pages, to create a safe and reliable environment on the Facebook pages. There are a number of methods to verify the FaceTrust, such as:

- Send the password resulting from the generator key by the one-way hash functions on the e-mail address which is located within the URL, in order to confirm the arrival of service to Facebook's pages for the service seekers'. Then send the activation key in the form of a password which is better than activating the link only to reduce the risks and threats.
- Authenticates the VIP by comparing the password sent via e-mail and the password in the database, if the password matches, it appears in an activation link which gets the trust service, and changes the personal settings on Facebook page.
- Setting up a Time Stamp mechanism to verify non-manipulation by hackers. Therefore, to enter a wrong URL for non-VIP users will enter a wrong URL, so it gives the activation link a particular time period, after the end of this period with no activation, the link will be automatically canceled completely, and also his registration on the database.

The activation operation is easy, free, and flexible; therefore the VIPs enter by the password sent to their email.

After any VIP user visits the FaceTrust page on Facebook, and enters the FaceTrust password, it validates this password, and the activation link page that appears, and then the user clicks on the activation link to update his page on the Facebook, therefore the trust logo appears inside the image; Fig. 11 shows the trust logo appears inside the VIPs image.

In addition, the FaceTrust controls viewing personal information on Facebook page, upon the terms that have been determined previously in the configuration process. The controlling process is completed by finding a third-party in the Facebook to support privacy protection, accordingly to create a special system of protection to achieve the needs of all VIPs.

Fig. 11 The trust logo inside the image of VIPs page

IV. Discussion

The new architecture mechanism FaceTrust that plays as a third party will be added on the Facebook in order to improve

the performance and find a solution to reduce the fake pages that exploit the VIPs names and cause distortions and abuses.

This application is limited to serving the VIPs that have a website, which documents their personal information on the webhosting and also offers violate privacy. Therefore, this issue became necessary for the VIPs to have their own account on Facebook.

The feasibility for this architecture which will be compared into Facebook through the service presence that gives a trust by the FaceTrust application or nonexistence of the FaceTrust. Notice that is the necessary existence of the FaceTrust service to give the trust of the Facebook pages distinguished by logo that approves a page ownership, which leads to reduce the fake pages and easily to discover the exploiting the names of VIPs.

The probable results used for the architecture FaceTrust are the increasing number of VIP subscribers in order to acquire service that provides trust on special pages**,** to distinguish personal pages from another fake page and easily recognized by the fans. Furthermore, increasing the confidence to use the FaceTrust architecture provides a free service for VIPs as well as the fans able to participate with favorite pages safely.

V. Conclusion

The increase of social networks and participants by internet users leading to increase the risks and threats in violation of privacy, explicitly for VIPs, so that the actual problem is the ability to create SNS pages without restrictions or verifying the identity of the applicant, thus using fake names for VIPs plus a photograph for the dissemination of rumors and distortion; Moreover, the increasing concern of the fans to join with favorite pages considering that they found many fake pages, so there is no solution to reduce the fake page problem, in addition to the lack of a mechanism to verify the identity of the owner account.

Therefore, the new secure architecture was found as an effective solution to reduce fake pages and possibility of recognizing VIP pages on SNS by the logo method which appears inside the profile photo. Hence the fans can recognize this page, as a result of using the way to authenticate and verify the personal information for VIP by already recorded information on their own website. So it is limited to serve only the VIPs which have an effective website, hence connecting the architecture and applied on Facebook, which are the most famous social-networking sites and also flexibility in dealing with the third party. The additional service on the FaceTrust application is the ranking service which provides reports the number of fans who joined to VIPs pages that use the FaceTrust application.

Acknowledgment

The authors would like to acknowledge financial support for this work from the Deanship of Scientific Research (DSR), University of Tabuk, Tabuk, Saudi Arabia, under grant no. 0072/1435/S

References

[1] A. Felt and D. Evans. "Privacy protection for social networking APIs". In *W2SP*, 2008..

[2] L. Fang and K. LeFevre. "Privacy Wizards for Social Networking Sites". WWW, 2010.

[3] Boyd, Danah M. and Ellison, "Nicole B. Social network sites: Definition, history, and scholarship". Journal of Computer-Mediated Communication, 13(1), 210-230,2007.

[4] D.Piscitello, & R. Mohan. "Is the WHOIS Service a Source for email Addresses for Spammers?". Journal of SSAC Fellow, 3 (1), 2007.

[5] Dugelay,J.,L,& Rey,C, (2002), "A Survey of Watermarking Algorithms for Image Authentication, EURASIP Journal on Applied Signal Processing", Hindawi Publishing Corp. New York, NY, United States1, January 2002.

[6] Ellison, N. B., Steinfield, C., & Lampe, C. "The benefits of Facebook 'friends:' Social capital and college students' use of online social network sites". Journal of Computer-Mediated Communication, 12, (4), 1143-1168, 2007.

[7] E. Mills, "Facebook suspends app that permitted peephole,", 2008. (On-Line), available: http://news.cnet.com/8301-10784\3-9977762-7.html.

[8] E. Steel and G. A. Fowler, (2010) "Facebook in online privacy breach; applications transmitting identifying information," available: http://online.wsj.com/article/ SB10001424052702304772804575558484 075236968.html.

[9] Gahanna,A. In foxnews , The Official: Prince William's Facebook Page a Royal Fraud. Retrieved 11:21, July 14, 2011, (On-Line), available http://www.foxnews.com/story/0,2933,272593,00.html

[10] Gross, R., & Acquisti, A. "Information revelation and privacy in online social networks". Paper presented at the ACM Workshop on Privacy in the Electronic Society (WPES), Alexandria, Virginia, 2005.

[11] Harrenstien, K., Stahl, M., and E. Feinler, (1985). "NICNAME/WHOIS., Internet Engineering Task Force, IETF, from: http://www.ietf.org/rfc/rfc954.txt

[12] Kelly, D. In IrishCentral.com, Irish billionaire to sue Facebook over fake profile pages, Claims social networking site has refused to take down bogus sites. Retrieved 10:21, July 14, 2011, (On-Line), available http://www.irishcentral.com/news/Irish-billionaire-to-sue-Facebook-over-fake-profile-pages-122794584.html

[13] Manuel .E., Andreas .M., Christopher ,K., and Engin. K., (2011), PoX: Protecting Users from Malicious Facebook Applications, 3rd IEEE International Workshop on Security and Social Networking (SESOC), Seattle, WA.

[14] Persits, P. In 15seconds , "AES, Protecting Passwords with a One-way Hash Function.htm", Retrieved 11:15, July 17, 2011, (On-Line), from http://aspnet.15seconds.com/feedback/ /AES/Protecting Passwords with a One-way Hash Function.htm.

[15] S. Kelly,. "Identity 'at risk' on facebook,", 2008. (On-Line), available: http://news.bbc.co. Uk/2/hi/programmes/click online/7375772.stm,.

[16] Strickland.J,. In Howstuffworks , How Facebook Works, Facebook Applications 2:11, July 21, 2011, (On-Line), available http://computer.howstuffworks.com/internet/socialnetworking/networks/facebook2.htm

[17] T. Berners-Lee, L. Masinter, and M. McCahill . "RFC 1738 Uniform Resource Locators (URL)," Dec. 1994. Available at http://www.w3.org/Addressing/rfc1738.txt

[18] V. Shah, . "Fair Trade Awareness through Social Networking Mediums and an Insight into Collaborative Filtering , Report is submitted as part requirement for the MEng ,pp 18.

[19] Wang, X., Yin, Y.L.and Yu, H. ,(2005), Finding Collisions in the Full SHA-1. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 2-3., Heidelberg

[20] Whois,. In checkurl , Whois: amrkhaled.net Find Domain Names www. amrkhaled.net Retrieved 7:51, July 10, 2011, (On-Line), available http://www.checkurl.info/whois.php?query=amrkhaled.net

[21] W. Luo, Q. Xie, and U. Hengartner, . "Facecloak: An architecture for user privacy on social networking sites," in CSE (3). IEEE Computer Society, Vancouver, BC, pp. 26–33, 2009.

[22] Zhu.Y., Zexing. H., Wang.H., Hongxin. H., and Gail-Joon .A. , (2010),A Collaborative Framework for Privacy Protection in Online Social Networks, In Proceedings of the 6th International Conference on Collaborative Computing, Chicago, Illinois, USA, October 9-12, 2010.

[23] M. Sato. Creating next generation cloud computing based network services and the contributions of social cloud operation support system (oss) to society. In Proc. of IEEE WETICE, pages 52–56, 2009.
[24] K. Chard, S. Caton, O. Rana, and K. Bubendorfer, "Social cloud: Cloud computing in social networks," in *IEEE CLOUD'10*, 2010, pp. 99–106.
[25] N. F. Shilbayeh, B. Abuhaija, Z. Alqudsy. Combined DWT-CT Blind Digital Image Watermarking Algorithm, World Academy of Science, Engineering and Technology, Vol:7 pp06-21, 2013.