A New Secure Architecture for Trust and Privacy on Social Network Sites

By

Mohmmad Hamed Allymoun

Supervisor

Prof. Nidal Shilbayeh

A Thesis Submitted in Partial Fulfillment

Of the Requirements for the Master Degree in

Computer Science

Faculty of Information Technology

Department of Computer Science

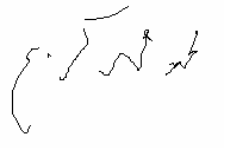
Middle East University

August, 2011

AUTHORIZATION FORM

إقرار تفويض

أنا محمد حمد الليمون أفوض جامعة الشرق الأوسط بتزويد نسخ من رسالتي للمكتبات أو المؤسسات أو الهيئات أو الأفراد عند طلبها.

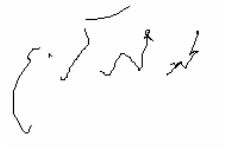


التوقيع:

التاريخ: 1 /11 2011

Authorization statement

I, Mohmmad Hamed Allymoun, Authorize the Middle East University to supply a copy of my Thesis to libraries, establishments or individuals upon their request.

Signature: 

Date: 1 /11 /2011

COMMITTEE DECISION

This is to certify that the thesis entitled "**A New Secure Architecture for Trust and Privacy on Social Network Sites**" was successfully defended and approved in August / 2011.

Examination Committee Members: **Signature**

Prof. Nidal Shilbayeh

Professor,Computer Science Department

(Middle East University)

Dr. Hazim A. Farhan

Department of Computer Science

(Middle East University)

Dr. Ghassan Issa

Faculty of Information Technology

(Petra University)

ACKNOWLEDGMENTS

In the Name of Allah

I would like to thank my supervisor Prof. Nidal Shilbayeh for his support, encouragement, proofreading of thesis drafts, and helping me throughout my thesis, and so putting me on the right track of Cryptography and Computer Security field. I thank the Information Technology Faculty members at the Middle East University for Graduate Studies. I thank my family for their continuous support during my study. I would also like to thank all my friends for their support during writing my thesis.

Table of Contents

Chapter One: Introduction..…… …1

1.1 Overview……..……2

1.2 Problem Definition ……..…....6

1.3 Objectives ……..……..…….7

1.4 Motivation ……..…...8

1.5 Thesis Organization……..…9

Chapter Two: LITERATURE SURVEY AND RELATED WORK…..……...…10

2.1 Overview……..…… ……11

2.2 Literature Survey……..…13

2.2.1 Uniform Resource Locator (URL)……..…….…13

2.2.2 WHOIS URL ……...…….……...…….…….13

2.2.3 Facebook Platform ……..…….…….……...15

2.2.3.1 Apps on Facebook.com …….……..…….……..……..15

2.2.3.2 Facebook Query Language (FQL)……..…..……..……..16

2.2.4 Watermark & Hash function …….……..17

2.2.4.1 Watermark…….……17

2.2.4.2 Hash function…….…….…….……18

2.2.4.2.1 One-way Hash Functions ……..…….……...…18

2.2.4.2.2 SHA-1 …….…….……18

2.3 Related work. …….…….…….……20

2.3.1 PoX: Protecting Users from Malicious Facebook Application ……...……..20

2.3.2 A Collaborative Framework for Privacy Protection in Online Social Networks ……..……....21

2.3.3 FaceCloak: An architecture for User Privacy on Social Networking Sites…….....22

Chapter Three: THE ARCHITECTURE OF FACETRUST…….……..…..24

3.1 Overview ……..……..……..…...25

3.1.1 FaceTrust Architecture ……..…..26

3.1.2 Principles of FaceTrust Design ……...……..…….28

3.2 Social networking & VIPs Users ..…….……...……..…….30

3.3 FaceTrust ……33

3.3.1 Configuration process …….…..……...36

3.3.2 Registrations process……39

3.3.2.1 Electronic Authentication…….…….……40

3.3.2.2 Registration Information…….…...……43

3.3.2.3 Stored Databases……..…….……45

3.3.2.4 Encryption……..……..…...……..46

I. Generating password……...……..…...……46

II. Trust logo process…….....……..49

3.3.3 Activation &verification……..……...50

Chapter Four: Analysis of the Architecture FaceTrust and Case Study ...…….….52

4.1 Overview……..……..…53

4.2 Case Study …….……..……..……..…..54

4.2.1 Problem and solution.……..……..…….…….....56

4.2.2 Challenges and Restrictions ……..……...…60

4.2.2.1 Challenges facing the use URL …….……..……..……...60

4.2.2.2 Challenges facing the trust logo ……..…..……63

4.2.2.3 Challenges facing the lost password …….…….…..……64

4.2.3 Scenario ……..……..65

4.3 Discussion …….…….……..……71

Chapter Five: Conclusion & Future Work …….…….74

5.1 Overview…….……...…75

5.2 Conclusion……75

5.3 Future Works……77

References……..78

List of Figures

Figure 2-1: axes of the Literature Survey & Related Work……...…….……..……12

Figure 2-2 the configuration screen and specify a Canvas Page and Canvas URL (2011)……..…….……..15

Figure 2-3: Data-flow in Facebook by PoX (2011)……...…….……..21

Figure 2-4: The system architecture for a private OSN (2010)…….…...…….22

Figure 2-5: Architecture of FaceClock (2009)…….……..…23

Figure 3-1: FaceTrust Architecture …….……...…27

Figure 3-2: Who is trusted?……..…….30

Figure 3-3: Some examples of community VIPs……..……31

Figure 3-4: the main processes of the FaceTrust architecture ..…….…….33

Figure 3-5: The Main Processes FaceTrust …….……....…….35

Figure 3-6: Applications Added to Facebook as a Third party (2011)…….…….38

Figure 3-7: Request for Permission (2011)……..…….38

Figure 3-8: Parts of the Registration Process……..…..….40

Figure 3-9: Important information necessary for the registration phase ……..….44

Figure 3-10: Process Generator Key ……...….48

Figure 3-11: Hashed Password by SHA-1……...…….48

Figure 3-12: Image processing using watermarking to produce trust logo……..…49

Figure 3-13: The Trust logo inside the image of VIPs page…….…..…….…….51

Figure 4-1: FaceTrust Application Homepage …….55

Figure 4-2: Facebook Signup Page …….……..56

Figure 4-3: : Search Results for a Facebook page ..…….……57

Figure 4-4: Example of Fake Pages for (Dr. Amr Khaled).…….…….58

Figure 4-5: FaceTrust Ranking Application ...…….…….59

Figure 4-6: Search results in Facetrust Application…….…….64

Figure 4-7: Facebok Login …….…….65

Figure 4-8: FaceTrust application link in advertisements bar …….…….66

Figure 4-9: FaceTrust Application page …….…….66

Figure 4-10: FaceTrust Home page……..…….…….……..…….67

Figure 4-11: Permission request window……..…….……..….67

Figure 4-12: Entering the website address For registration...…….……..….68

Figure 4-13: Random password sent by password generation From FaceTrust application …….…….……..…….68

Figure 4-14: Entering the password that sent to user Mail ……..…….69

Figure 4-15: FaceTrust page after validate the password..…….……..…….69

Figure 4-16: An example of a participated page in the trust service ……..….70

Figure 4-17: Example how the trusted page viewed in the results ……..….73

List of Abbreviations

API	**Application Programming Interface**
APP	**Application**
CSS	**Cascading Style Sheets**
FMBL	**Facebook Markup Language**
FQL	**Facebook Query Language**
GCC	**Group-oriented convergence cryptosystem**
HTML	**Hypertext Markup Language**
ID	**Identifier**
OSN	**Online Social networking**
SHA	**Secure Hash Algorithm**
SNS	**Social networking Site**
SQL	**Structured Query Language**
TCP	**Transmission Control Protocol**
TOS	**Terms of Service**
URL	**Uniform Resource Locator**
VIP	**Very Important Person**

ABSTRACT

In recent times the interest in internet users to social networking has increased, so it became the appropriate environment for media organizations, political personalities, artists and famous social figures for interaction with admirers and friends. This group is called "VIP," where the presence of a personal page on Facebook on the website is currently important for them, especially if they have their own website. The real threat 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, but unfortunately, there is no effective mechanism that gives trust in dealing with these pages and verify the real identity of the owners page, as well as increase level of privacy protection. 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. The indication trust on the personal page of a subscriber in the trust service is the appearance of the trust-logo appears within the photograph profile on Facebook, through which friends and admirers can easily recognize and distinguish it from other fake ones, in addition to privacy protection.

As a result, the general significance of the new security system is that it secures and provides trust to the personal pages of the increasing number of VIP subscribers on Facebook who seek such a service. Further, it can help to discover fake page, reduce crimes of personality-theft, protect the privacy, and increase the sense of trust and satisfaction by friends and admirers in interacting with Facebook.

الخـــــــــــــــلاصة

في الآونة الأخيرة ازداد اهتمام مستخدمي شبكة الانترنت لشبكات التواصل الاجتماعي , بحيث أصبحت بيئة مناسبة للمنظمات الإعلامية والشخصيات السياسية والفنانين و الشخصيات الاجتماعية المشهورة للتواصل مع المعجبين والأصدقاء , و هذه المجموعات يطلق عليها "الشخصيات المهمة " حيث أصبح وجود صفحة شخصية على فيسبوك امراً مهما في هذا الوقت مع وجود موقع الكتروني خاص بهم , لذلك فان التهديد الحقيقي لهذه الصفحات هو انتهاك الخصوصية وانتحال شخصية عن طريق إنشاء صفحات وهمية تستغل أسماءهم وصورهم لجذب ضحايا ونشر الأكاذيب, بحيث لا توجد آلية فعالة تعطي الثقة في تعامل مع هذه الصفحات و التحقق من الهوية الحقيقية لصاحب الصفحة , مع رفع مستوى الحماية للخصوصية .

إن المعمارية المقترحة تعمل كطرف ثالث يتم أضافته على الفيسبوك ليقدم خدمة الثقة و الخصوصية على الصفحات الشخصية للشخصيات المهمة , من خلال آلية تعمل على التأكد من الهوية الحقيقية لطالب الخدمة وذلك بالتوثيق الالكتروني للمعلومات الشخصية من خلال المعلومات المخزنة في الأساس في محتوى الموقع الالكتروني الخاص بهم ,وتكون دلالة الثقة على الصفحة الشخصية للمشترك في خدمة الثقة هو ظهور شعار الثقة على الصورة الشخصية للصفحة على فيسبوك. والتي من خلالها يسهل استدلال المعجبين والأصدقاء مع سهولة تمييزها من بين الصفحات الوهمية مع حماية الخصوصية .

وفي النتيجة فان التصور العام لنظام الأمني الجديد هو ازدياد عدد المشتركين وطالبي خدمة الثقة من قبل الشخصيات المهمة بالاشتراك , كجهة تؤمن وتعطي الثقة لصفحاتهم الموجودة على الفيسبوك , وتساعد على اكتشاف الصفحات الوهمية والحد من جرائم انتحال الشخصية,و أيضا يزداد الشعور بالثقة و الارتياح من قبل المعجبين في التعامل والتراسل.

Chapter One

INTRODUCTION

Chapter One

Introduction

1.1. Overview

The social networking is a new way to communicate with users who can include all services blogs, tweets and post. There are actually large numbers of artists and media organizations that take advantage of social networking, so that social media found a new type of conversation with existing customers, and also publish news and accept opinions. The social networking focuses on building communities, and connecting people of similar thoughts, hobbies, and interests. The groups of users often have common interests called friends. It can exchange information from texts, pictures and videos between them.

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 for friendship and create groups on social networking.

Ellison et al., (2007) said that a social network site 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 (Boyd & Ellison, 2007; Ellison, Steinfield, & Lampe, 2007; Gross & Acquisti, 2005). Thus, a

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 a method available 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.

Boyd, Danah M. and Ellison, Nicole B. (2007) said that the main technical underpinnings of SNS infrastructures and services include Web 2.0 technologies, service-oriented software, caching, database and content distribution technologies. From a technical point of view, SNS sites provide APIs, software frameworks and open-source platforms that enable application developers to build applications and manipulate their content. The SNS allowed users to connect with both friends and strangers alike, and it depends on how much information the users want to share. It becomes very beneficial in a closely bounded system like college or workplace, where individuals may decide to be friends with individuals pertaining to the same system. Even though SNS is a decent means to meet and interact with new people, a lot of users just want to communicate with the people they know and take advantage of the resources that the website has to offer.

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.

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.

KELLY,D.,(2011) the Renowned Irish multi-millionaire JP McManus is suing Facebook for allegedly failing to remove three fake profile pages claiming to be him. McManus, who is known for his privacy, is also seeking declarations that Facebook's alleged failure to remove the accounts is an unlawful breach of his constitutional rights. He is also seeking damages for defamation, malicious falsehood, fraudulent misrepresentation and negligence.

GAHANNA, A., (2007) The U.K. Telegrapher reported that the prince had a Facebook page and 44 friends under the name William Wales. Facebook removes any content that is in violation of our terms of use, including fake profiles," a Facebook spokeswoman told FOXNews.com. "After investigating the profile for William Wales, we found that it was a fake profile and we removed it from the site. We encourage users to report any violations of our terms.

A New Secure is applied on Facebook Platform that easily deals with the third party and cooperates with them, and the ability to control the change settings on Facebook platform.

Note: A New Secure will be named as FaceTrust.

1.2. Problem Definition

There are many problems related to the social networks which differ according to the use and dealing with others, which affect the behavior of most communities, because of the growing number of users and the large amounts of data handled, which leads to increase risks and threats, especially in the trust and privacy, through using illegal ways and smart methods by vandals in order to violate privacy and trust reduction.

Trust is the missing element in social networking so that creating an account is based on good intentions. There is no legal contract to make sure of the real identity of the owner's account. Accordingly, there is a disadvantage of wrong exploitation and emergence of fake pages by using names of VIPs to publish lies and rumors, as a result of increasing the concern in dealing with fans and the favorite pages on social networking.

The following problems have been identified:

1- The inability to verify and make sure of the real identity of the owner's account on social networking, which means that there're no specific properties that may be added on the personal page. This may lead to one infer these pages could be fake pages, leading to a distrust in dealing with them.

2- Creating accounts easily on social networking, so there is no mechanism for documenting information for the page owner and establish accounts on the principle of trust, which leads to easily exploitation of VIPs names and photographs to attract the attention of friends and admirers, and this in turn leads to spread lies and rumors without permission from the VIPs.

3- The increasing number of fake pages on Facebook of the VIPs, which makes it riskier to the VIPs and admirers to interact together safely.

1.3. Objectives

The main objectives of this research are the following:

1) Design of a third party FaceTrust which may be added to the Facebook to solve all of the above-mentioned problems easily without complications, to create safe and trusted personal pages on social networking, which will work cooperatively with Facebook to provide a trust service on the VIPs pages.

2) Develop a mechanism for electronic authentication of personal information of the VIPs, who use the Facebook, and to get the information related to the VIP from their website, during documenting, such information which is already recorded on the webhosting, in order to confirm the identity of the true seeker's service.

3) Find distinctive logo that appears inside the profile image of the VIP on Facebook, so that it indicates to participate in the FaceTrust service. This leads to ease of the inference fans to the favorite pages, then the trust logo is distinct and attracts fans and reduces the fake pages for VIPs on Facebook.

1.4. Motivation

The main aim of the New Secure Architecture is to find a third party connected with Facebook to improve performance of privacy and to find a solution to the problem of the fake pages by giving trust to the pages of the VIPs, in order to become a distinctive and unique from, easy inferred by fans and friends, through verification and make sure of the identity of the VIPs by getting personal information in the website. The logo appears on the profile image.

The general perception of FaceTrust is the increased number of subscribers and service seekers trusted by VIPs, it helps to discover the fake pages that exploit the names and photographs of VIPs to broadcast rumors and news exploited illegally.

Either the fans or friends get a feeling trust and satisfaction in dealing with pages and conversation with VIPs participating in the service FaceTrust, in order to allow evaluation of pages on Facebook through knowing the real number of the fans that benefit media issues to VIP. Consequently, there is reduced dispersion of fans and friends jointly with fake pages that used the methods of social attack.

Previous knowledge VIP-winning service that FaceTrust will be responsible for any information published on the personal page, so that the VIP is under the legal accountability for any abuse published from this page.

1.5. Thesis Organization

In addition to this chapter, there are four other chapters. Chapter 2 describes the security of protection of trust and privacy to social networking and major terminologies relevant to the contents of the contributions which are made. Related work relevant to social network security is investigated in order to assist the conduction of this research. Through the addition of a third party on Facebook to improve the performance of the security, and find solutions to problems related to the architecture of Facebook in addition to improve the effectiveness. Chapter 3 describes the design of the proposed New Secure Architecture, called FaceTrust to give trust for profile pages through the mechanism of verification and documentation of personal information within the URL and give the Trust logo to pages.

Chapter 4 describes the analysis of the efficiency of the proposed scheme aspects of security and performance requirements, discussion and the results of the analysis.

Finally, Chapter 5 contains the conclusion and the future work of this thesis.

Chapter Two

LITERATURE SURVEY AND RELATED WORK

Chapter Two

Literature Survey and Related Work

2.1 Overview

In recent years there is an increased interest in using social networking in all types of fans which has created a communicative environment to achieve the principles of social networking; ccordingly, there has been an increased number of studies and research on social networking that aim to find a perfect structure, free of defects and problems. Those studies and research have focused on several issues, including (architecture and structure of SNS, privacy, security and protection, social behaviors, threats and risks).

The most important attention in such studies and research was on the behavioral side of the privacy of users on social networking to achieve results that help protect privacy of the participants which is considered the weak point of threatening in the future of SNS. This research is focused on how to find a revision of architecture types of social networking, such as encryption of messages and mechanisms for the protection of privacy.

Studies and research have proven the feasibility of a third party within the social networking, while results increased the security level and protection with an improvement of the social-networking behavior.

Research and recent studies have focused on FaceTrust to solve any problem concerning the protecting of trust of SNS pages, especially VIP, and find a mechanism to distinguish between social-networking pages and the easily identified by trust logo. Following are several related works, which focused on finding problems solutions facing users of social networks through the addition a third party on SNS and interact with them successfully.

The axes of the literature survey to complete the process, give the trust to the VIP pages on Facebook, and find an integrated solution to get the architecture which can achieve the objectives and solve the problem of trust;These axes are the following:

1- URL

2- Facebook

3- Watermark & Hash funcation

The figure 2-1 shows the axes of the literature survey to achieve the targets.

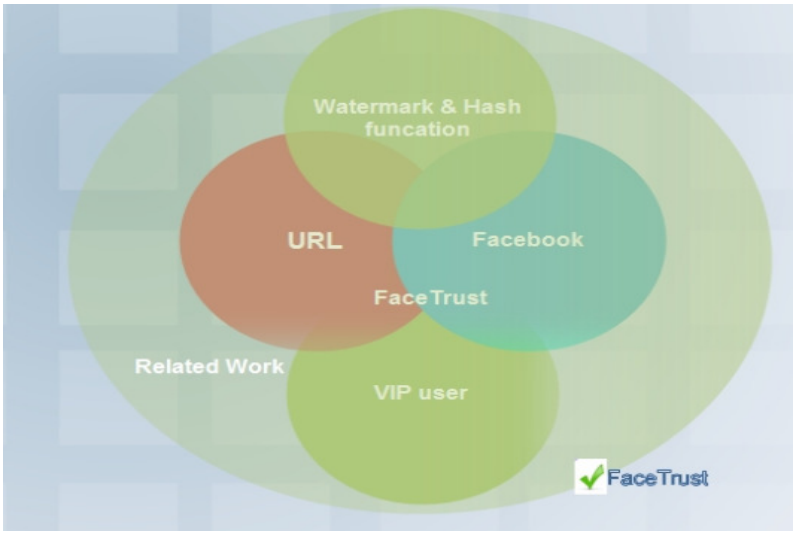


Figure 2-1: axes of the literature survey & Related Work

2.2 Literature Survey

2.2.1 Uniform Resource Locator (URL)

T.Berners-Lee, Masinter, & McCahill(1994) said that URLs are used to `locate' resources, by providing an abstract identification of the resource location. Having located a resource, a system may perform a variety of operations on the resource, as might be characterized by such words as `access', `update', `replace', `find attributes'. In general, only the `access' method needs to be specified for any URL scheme. In most URL schemes, the sequences of characters in different parts of a URL are used to represent sequences of octets used in Internet protocols. For example, in the ftp scheme, the host name, directory name and file names are such sequences of octets, represented by parts of the URL. The URL schemes that involve the direct use of an IP-based protocol to a specified host on the Internet use a common syntax for the scheme-specific data, that any user name or password is different; There are many occasions when URLs are included in other kinds of text; examples include electronic mail, USENET news messages.

2.2.2 WHOIS URL

Harrenstien, K., Stahl, M., and E. Feinler, (1985) said that WHOIS is a TCP-based transaction-oriented query/response protocol that is widely used to provide information services to Internet users. While originally used to provide "white pages" services and information about registered domain names, current deployments cover a much broader range of information services. The protocol delivers its content in a human-readable format. This document updates the specification of the WHOIS protocol,

For D.Piscitello, & R. Mohan, (2007) domain name registration information is often referred to as "WHOIS data". This loose terminology perpetuates a misconception that all registration records are held in a centralrepository. In practice, domain name registration information is stored in multiple databases maintained by registries and registrars. These databases can be queried through interfaces provided by registrars and registries. Two forms of access are provided:individual and bulk record access. Query-based WHOIS access registries, and resellers provide access to individual domain name registration information through one or more forms of query-response applications. Registries commonly support individual domain name queries via a world wide web browser interface. Many commercial and community web portals also provide a webbased WHOIS access by accepting queries from an end user, forwarding these to a registrar or registry, and directing the response from the registrar or registry back to the end user. A successful query to a “thick” registry will return the following information, referred to as the Domain Record:

- Domain Name ; Domain ID ; Sponsoring Registrar; Sponsoring Registrar IANA ID ; Domain Status.

· Registrant; Administrative ; Technical and Billing Contact Information including: ID , Name , Organization , Address , Geographic Location Code, Phone Number, Facsimile Number, Email.

- Name Server(s); Created by Registrar; Last Updated by Registrar; Domain Registration Date ; Domain Expiration Date ; Domain Last Updated Date

A successful query to a “thin” registry (such as .COM) will return the following information.

2.2.3 Facebook Platform

2.2.3.1 Apps on Facebook.com

Strickland.J, (2011) Apps on Facebook.com are loaded into a Canvas Page. A Canvas Page is quite literally a blank canvas within Facebook on which to run your app. You populate the Canvas Page by providing a Canvas URL that contains the HTML, JavaScript and CSS that make up your app. When a user requests the Canvas Page, this results in your app being displayed within the standard Facebook chrome.

To set up your Canvas Page and Canvas URL ,you must first register your Facebook app and enter in your basic app information. With that complete, click the "Facebook Integration" figure 2-2 shows the configuration screen and specify a Canvas Page and Canvas URL.

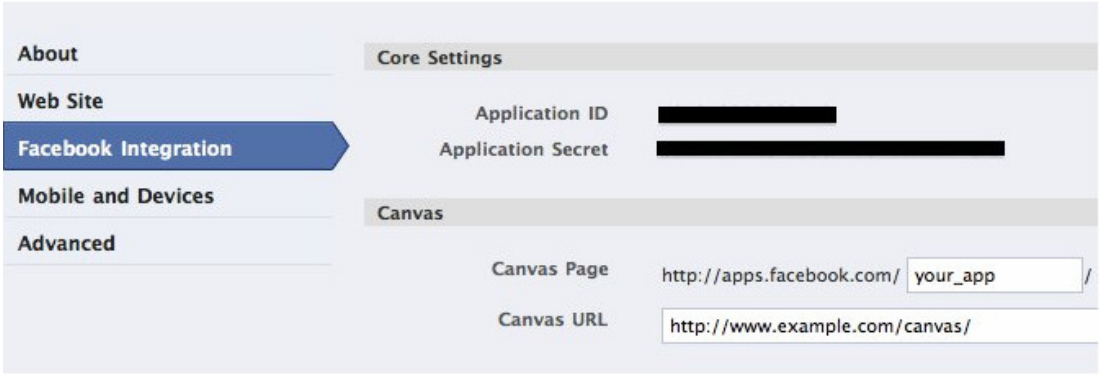


Figure 2-2: the configuration screen and specify a Canvas Page and Canvas URL (Strickland.J, 2011)

In order to gain access to all the user information available to your app by default (like the user's Facebook ID), the user must authorize your app. We recommend that you use the OAuth Dialog for Apps on Facebook.com.

To drive more traffic to your app, we enable some channels automatically as people use your app. Once a user starts using your app, we create a bookmark to enable users to easily navigate back to your app from within Facebook. We also publish a usage story to notify their friends that the user has started to use your app. Lastly, your app is automatically added to the App Dashboard or Game Dashboard.

Every application has a space on Facebook called a canvas page, which developers can use however they wish. When a user clicks on an application icon, his or her web browser goes to that application's canvas page. Developers can include Web advertising on canvas pages, sell products using a Facebook-designed interface or simply share information with the user.

2.2.3.2 Facebook Query Language (FQL)

V. Shah, (2009) FQL is a SQL-style language whose primary purpose is to allow developers to interact with Facebook information. Facebook allows access to nine tables so that developers can query this information directly. Access is granted to information about users, friends, groups, events, photos, and albums. Although similar to SQL, there are a few restrictions. For example, SELECT statements can only be performed on one table at a time, and join queries are not allowed. As mentioned above, the API calls are merely wrappers for FQL queries. FQL has advantages over the API calls in that bandwidth and parsing overhead is reduced, and the number of data requests can be reduced in certain situations. FQL is more efficient as you can specify specific fields that you want to have included in the result set; API calls retrieve all the field data for a given record.

Facebook Query Language , (2011) the beauty in FQL is the ability to query any Facebook data just as you would from a SQL database. In the following query, we pull four different types of data from a single table (status) where the

user is me. When trying to do this yourself, you need to log into Facebook from your application and you also probably need to grant access to whatever data you want to pull. Due to the growing number of privacy concerns for social networks, most people have disabled most data to be shown to anyone and your application will therefore not be able to see it. However, once you log in and grant access, you can see all data that you grant access to.

2.2.4 Watermark & Hash function

2.2.4.1 Watermark

Alpvision,(2011) Digital Watermarking describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video or audio. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. The hiding process has to be such that the modifications of the media are imperceptible. For images this means that the modifications of the pixel values have to be invisible. Furthermore, the watermark must be either robust or fragile, depending on the application. By "robust" we mean the capability of the watermark to resist manipulations of the media, such as lossy compression (where compressing data and then decompressing it ,retrieving data that may well be different from the original, but is close enough to be useful in some way), scaling, and cropping, just to enumerate some. In some cases the watermark may need to be fragile. "Fragile" means that the watermark should not resist tampering, or would resist only up to a certain, predetermined extent.

2.2.4.2 Hash function

2.2.4.2.1 One-way Hash Functions

Persits, P. , (2011) A one-way hash function has many names. Among them are message digest, fingerprint, and compression function. A hash function is an algorithm that takes a variable-length string as the input and produces a fixed-length binary value (hash) as the output. The tricky part is to make this process irreversible, that is, finding a string that produces a given hash value should be very hard (hence the word "one-way"). It should also be hard to find two arbitrary strings that produce the same hash value.

2.2.4.2.2 SHA-1

SHA-1 is a cryptographic hash function designed by the National Security Agency and published by the NIST as a U.S. Federal Information Processing Standard. SHA stands for Secure Hash Algorithm. The three SHA algorithms are structured differently and are distinguished as SHA-0, SHA-1, and SHA-2. SHA-1 is very similar to SHA-0, but corrects an error in the original SHA hash specification that led to significant weaknesses. The SHA-0 algorithm was not adopted by many applications. SHA-2 on the other hand significantly differs from the SHA-1 hash function.

SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely-used security applications and protocols. In 2005, security flaws were identified in SHA-1, namely that a mathematical weakness might exist, indicating that a stronger hash function would be desirable. Although no successful attacks have yet been reported on the SHA-2 variants, they are algorithmically similar to SHA-1 and so efforts are underway to develop improved alternatives

For Wang, X, et al., (2005) the SHA-1 hash function produces a 160-bit message digest based on principles similar to those used by Ronald L. Rivest of MIT in the design of the MD4 and MD5 message digest algorithms, but has a more conservative design.

The hash function SHA-1 takes a message of length less than 264 bits and produces a 160-bit hash value. The input message is padded and then processed in 512-bit blocks in the Damgard/Merkle iterative structure each iteration invokes a so-called compression function which takes a 160-bit chaining value and a 512-bit message block and outputs another 160-bit chaining value. The initial chaining value is a set of fixed constants, and the final chaining value is the hash of the message.

2.3 Related work

2.3.1 PoX: Protecting Users from Malicious Facebook Application

Manuel, Andreas, Christopher & Engin , (2011) said that "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, an extension for Facebook that makes all requests for private data explicit to the user and allows him to exert fine-grained access control over what profile data can be accessed by individual applications. By leveraging a client-side proxy that is executed 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."

Using the Java programming is downloaded to the browser in the client-side and connected with a Facebook account, to act as a proxy filter executing the requests that are coming in and out between the Facebook and personal accounts, plus comparing the requests with the list of ACL (access control list) .So that requested within authorized in dealing with personal data can access pre-identified data opposite not allowed.

The PoX is working as a third party added on the architecture Facebook in order to increase the privacy and protection from exploitation, in order to solve the problem of access to the personal information by the third party directly without users knowledge and illegal exploitation to work for filter requests. And it also needed to get services the presence of the special browser and download extra program on the client-side, including the skill of the users in dealing with programming.

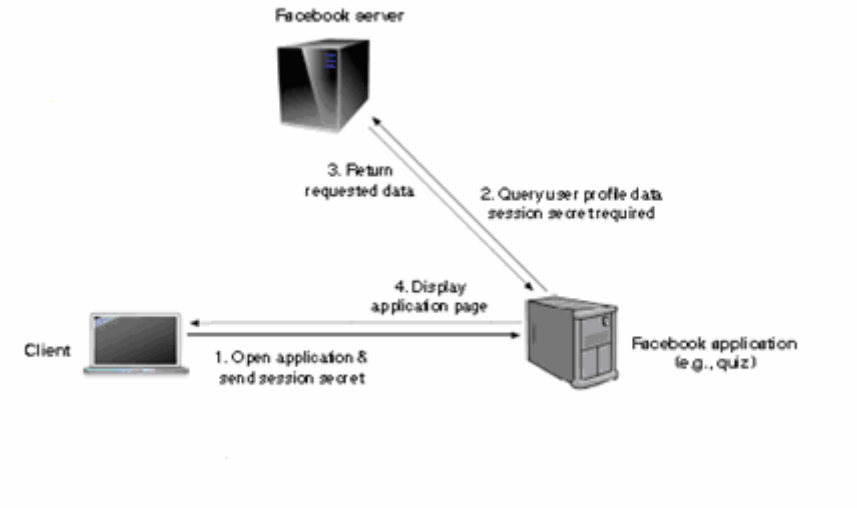


Figure 2-3: Data-flow in Facebook (Manuel, Andreas, Christopher & Engin , 2011)

2.3.2 A Collaborative Framework for Privacy Protection in Online Social Networks

Zhu, etal . (2010) said that "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 the authorized users. We propose 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".

The collaborative frame work is working as a third party added on Facebook architecture to encrypt the information sent within a group of trusted

people, so that the distribution of keys within the authority is determined by the administration, the mechanism of work sends information to a third party that has been encrypted and sent to the group. The benefit is to improve the performance of Facebook to protect information and encryption, so it needs administration and distribution of keys within a group.

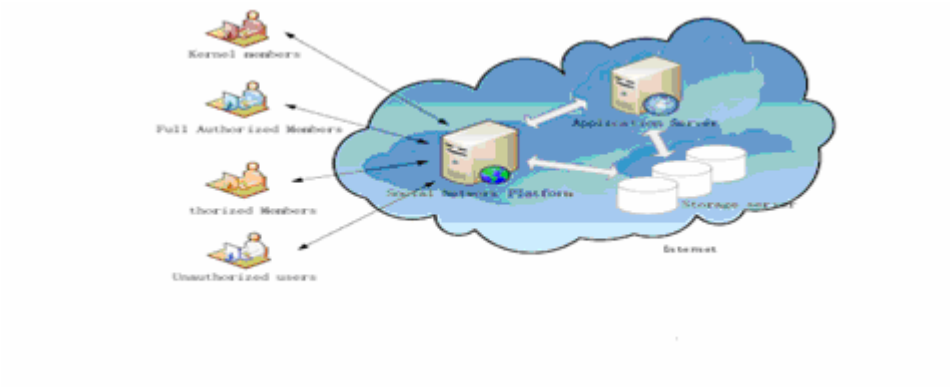


Figure 2-4: The system architecture for a private OSN (Zhu, etal. 2010)

2.3.3 Face Cloak: an architecture for User Privacy on Social Networking Sites

Luo, Xie., and Hengartner , (2009) " The FaceCloak 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 onceals a user's personal information, while allowing the user and his friends to explore Facebook pages and services as usual".

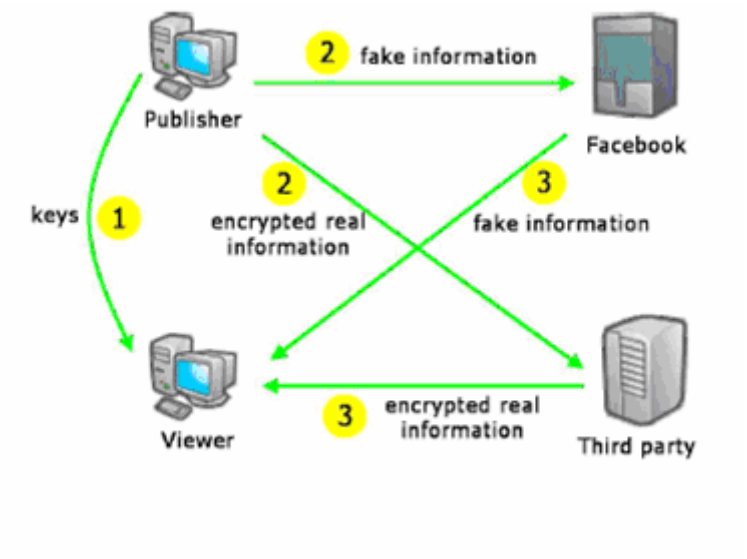


Figure 2-5: Architecture of FaceClock (Luo, Xie., and Hengartner , 2009)

The FaceCloak is close to the work of FaceTrust principle, as a third party whose information is encrypted and connected with Facebook. So that information is encrypted in order to produce fake information that is published on the Facebook pages, and also cannot decrypt this information and access only those who have the key. In addition, it finds an effective mechanism to increase the protection of information on Facebook, as a result to make sure that the use of a third party aimed at improving Facebook's performance.

Chapter Three

THE ARCHITECTURE OF FACETRUST

Chapter Three

THE ARCHITECTURE OF FACETRUST

3.1 Overview

This chapter presents the design of the FaceTrust architecture that gives trust and privacy to the SNS. 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. Note that dealing with the social networking environment is based on trust. In Figure 3-1 it shows the main parts to produce an integrated and effective system which achieves all the objectives of FaceTrust. The architecture could be built on existing social network platforms, such as Facebook, Orkut, MySpace, etc.

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. Facebook alone has over 81,000 third-party applications and allows external developers to create and launch their own applications. FaceTrust is considered as a third party, wherefore Facebook is the most appropriate site.

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

3.1.1 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.

Figure 3-1 shows the main operations on our model.

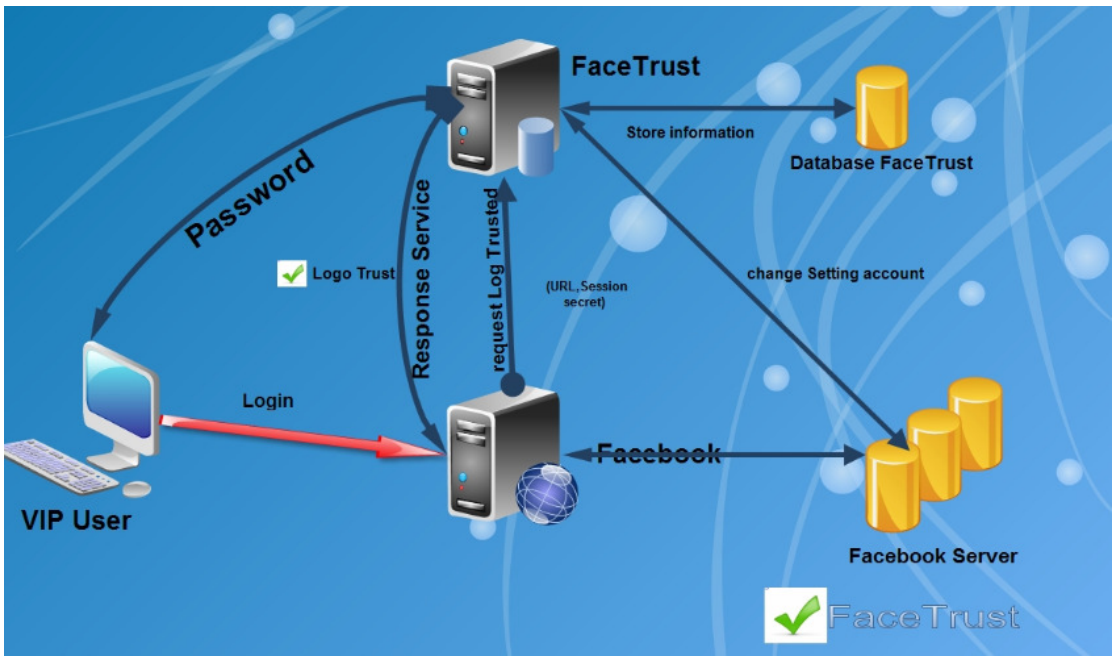


Figure 3-1: FaceTrust Architecture

The parts of FaceTrust Architecture:

1 - social networking & VIPs user.

2 – FaceTrust**.**

After studying the various existing solutions, one is led to believe that trust protection is the type of security technology that if it does not exist it would be exploited to threaten the reputation of the VIPs, who used the social networking. Therefore there are several reasons including unawareness of the VIPs such as, how to attract attention of fans to their pages and also Facebook's server-side vulnerabilities to find solutions for such threats. The FaceTrust architecture automates the process of trust protection.

3.1.2 Principles of FaceTrust Design

The design of FaceTrust is based on several principles:

1) 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.

2) 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. (Luo, Xie., and Hengartner , 2009). 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.

3) 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 softwares, and thus the VIPs users follow a number of procedures to authenticate information by their own URL.

4) 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.

3.2 Social networking & VIPs 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 figure 3-2. 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.

Figure 3-2: 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.

Figure 3-3: Some examples of community VIPs

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.

3.3 FaceTrust

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

Figure 3-4 shows the three processes.

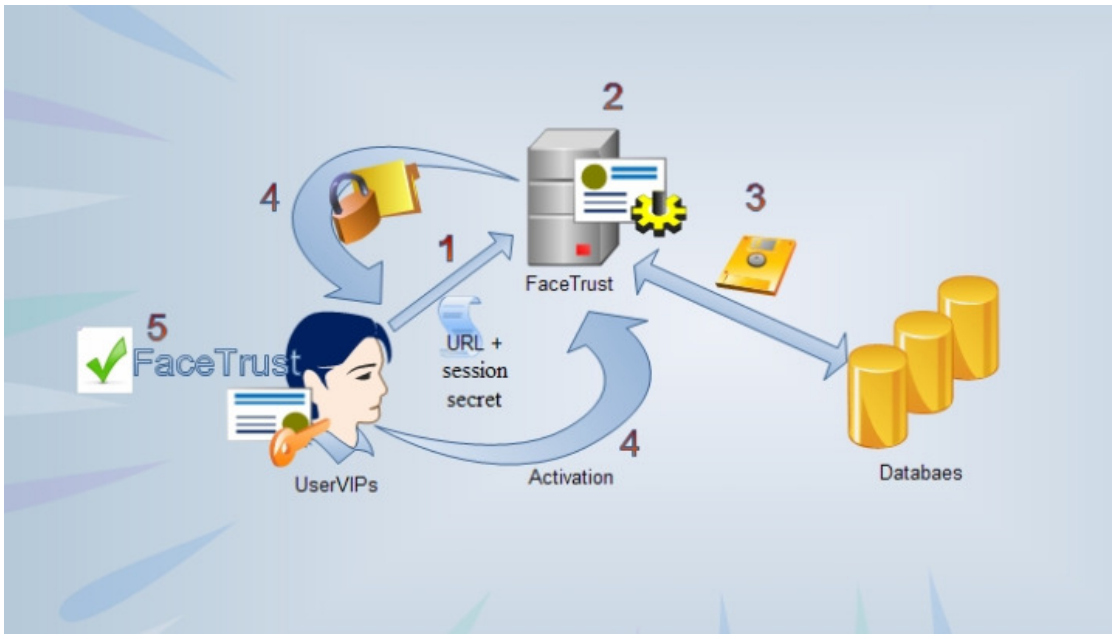


Figure 3-4: the main processes of the FaceTrust architecture

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.

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 WHOIS feature application which retrieves all the information contained within the URL. 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.

Figure 3-5 below shows the main processes of the FaceTrust.

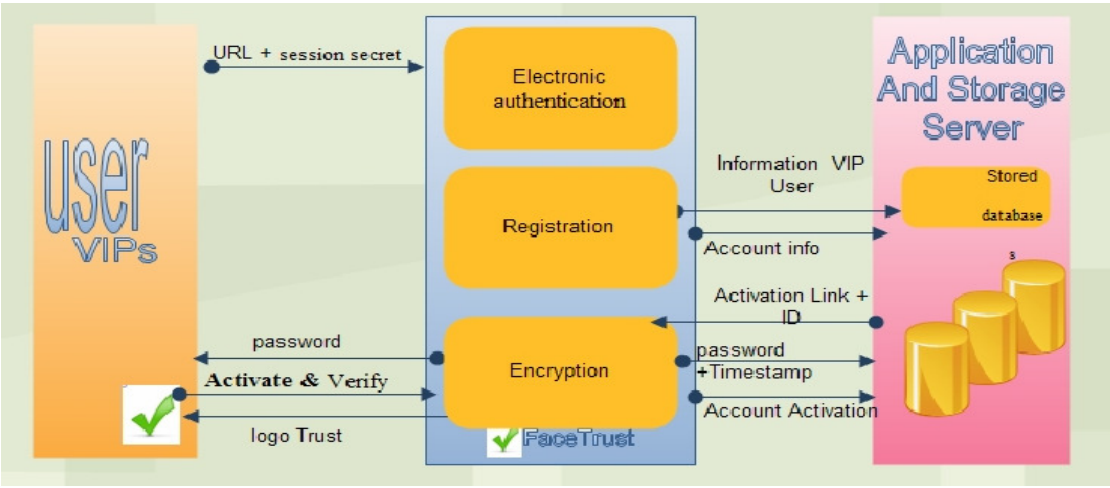


Figure 3-5: The Main Processes FaceTrust

3.3.1 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. Figure 3-6 shows some applications added on the Facebook as a third party, moreover, 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 procedures of the configuration processes are the following:

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

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

3- The permission request screen appears asking the user permission to access personal information, moreover, determine the privacy options that allow access through FaceTrust. Figure 3-7 shows screen request for permission.

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 of the registration process.

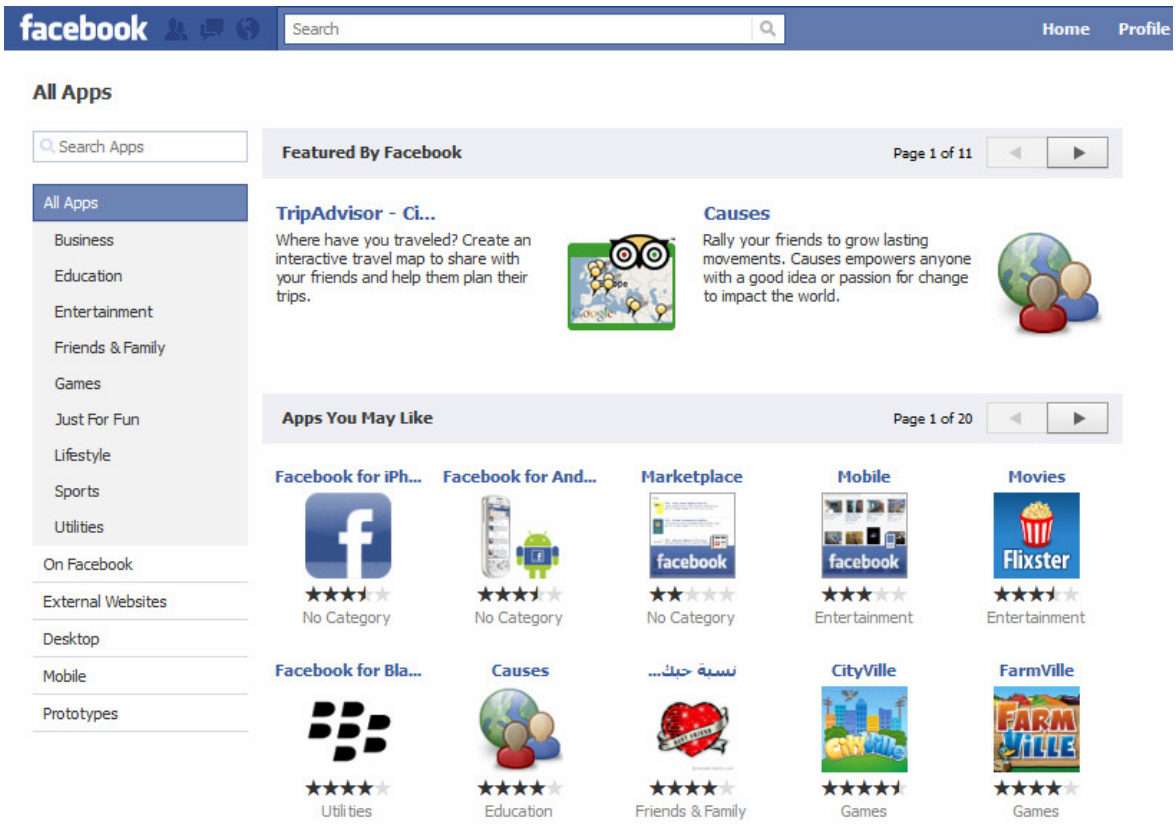


Figure 3-6: Applications Added To Facebook As a Third party (Markey &Barton ,2011)

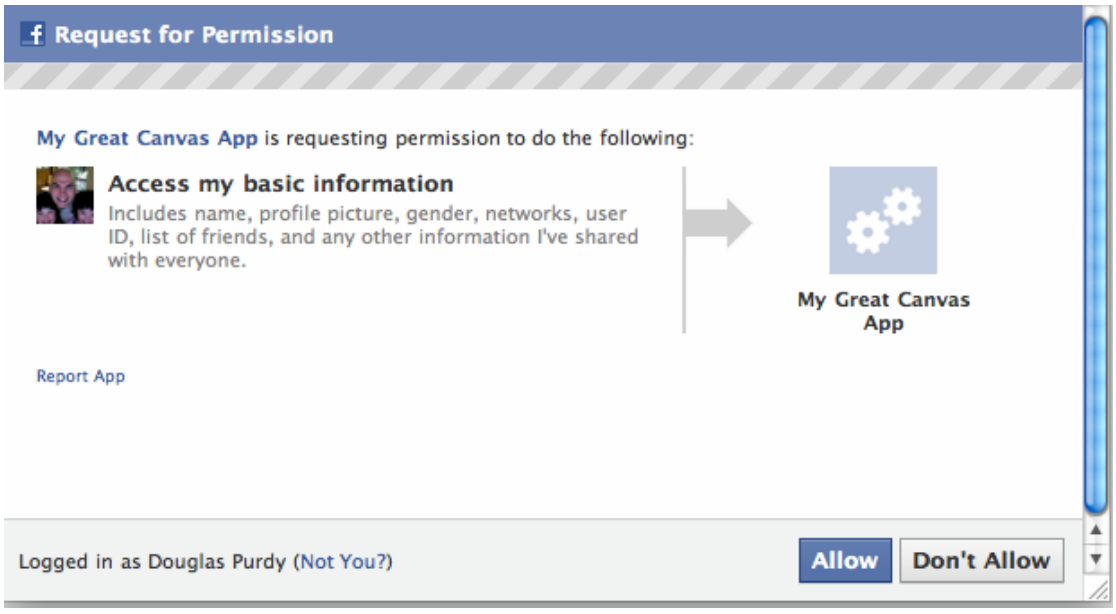


Figure 3-7: Request for Permission (Markey &Barton ,2011)

3.3.2 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.

Figure 3-8 shows a parts of the registration process, which is composed of four components as the following:

1 - Electronic Authentication

2 – Registration Information

3- Stored Databases

4 - Encryption

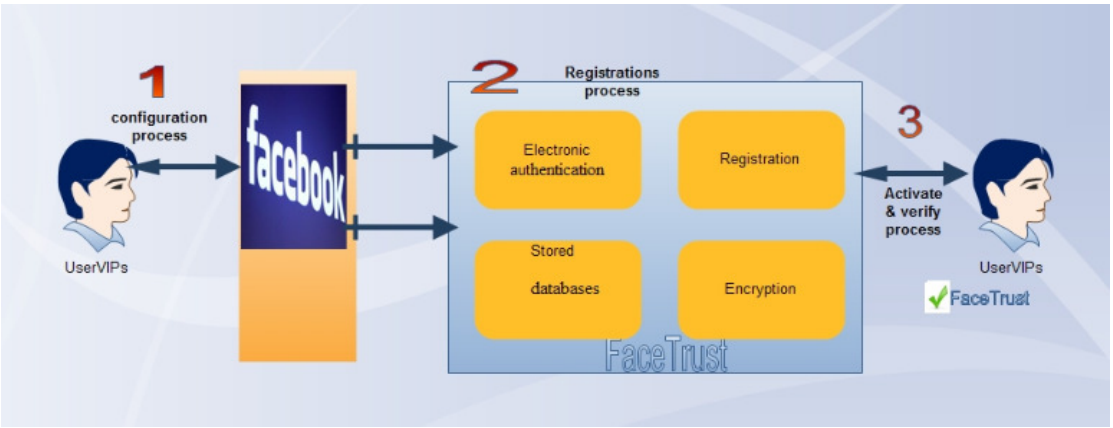


Figure 3-8: Parts of the Registration Process

3.3.2.1 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.

Electronic Authentication: the process to ensure the identity of persons dealing with the social networking through information and documentation obtained from the URL that was previously registered without the need of a paper-based registration step.

The following example 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 (Whois, 2011).

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://www.godaddy.com)
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.com
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

3.3.2.2 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.

Figure 3-9 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.

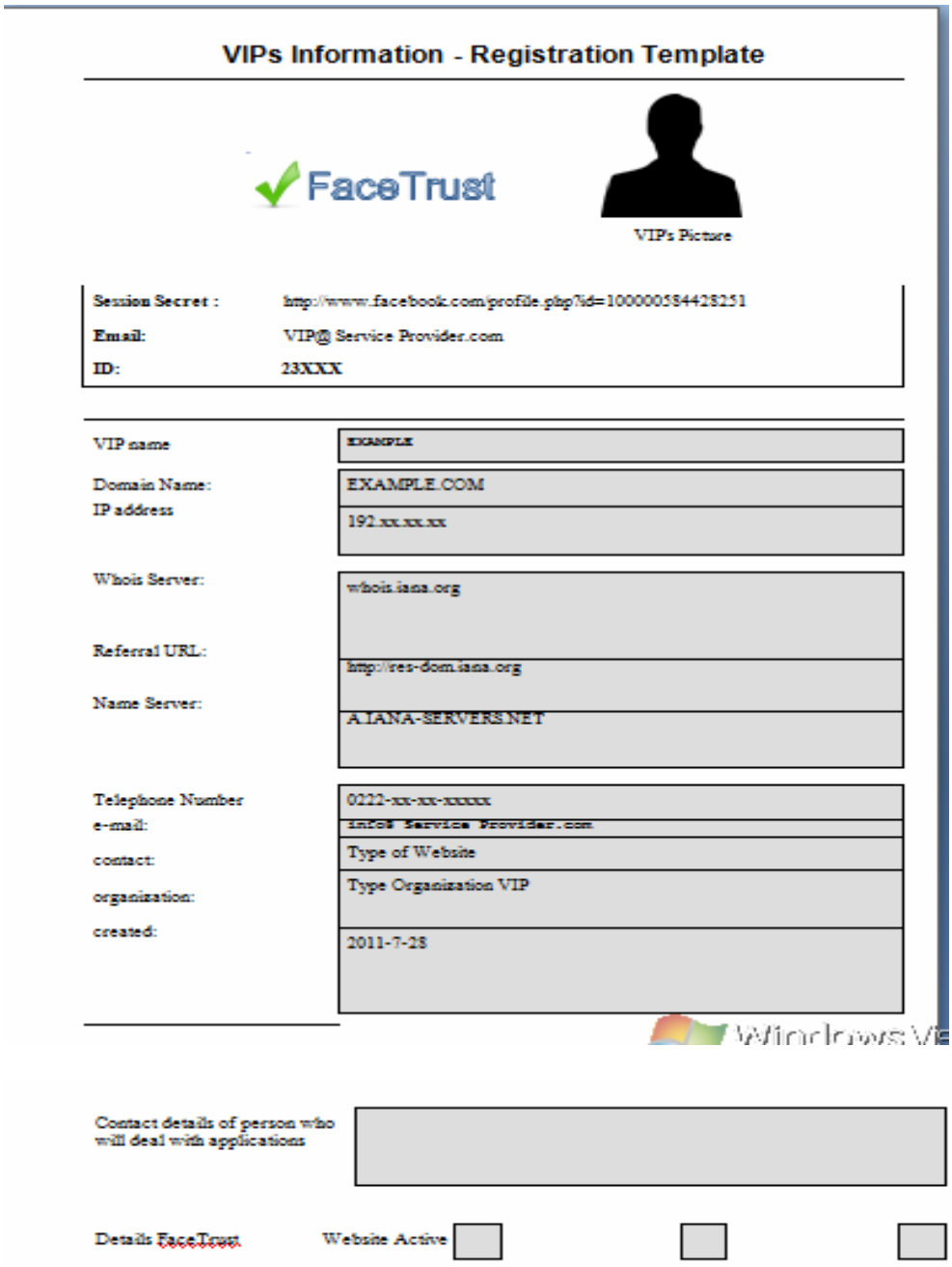


Figure 3-9: Important information necessary for the registration phase

3.3.2.3 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.

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.

3.3.2.4 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.

I. Generating password

The password is one of the essential requirements that must be available in the architecture, 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, including:

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

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

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.

Figure 3- 10 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. 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. Figure 3-11 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.

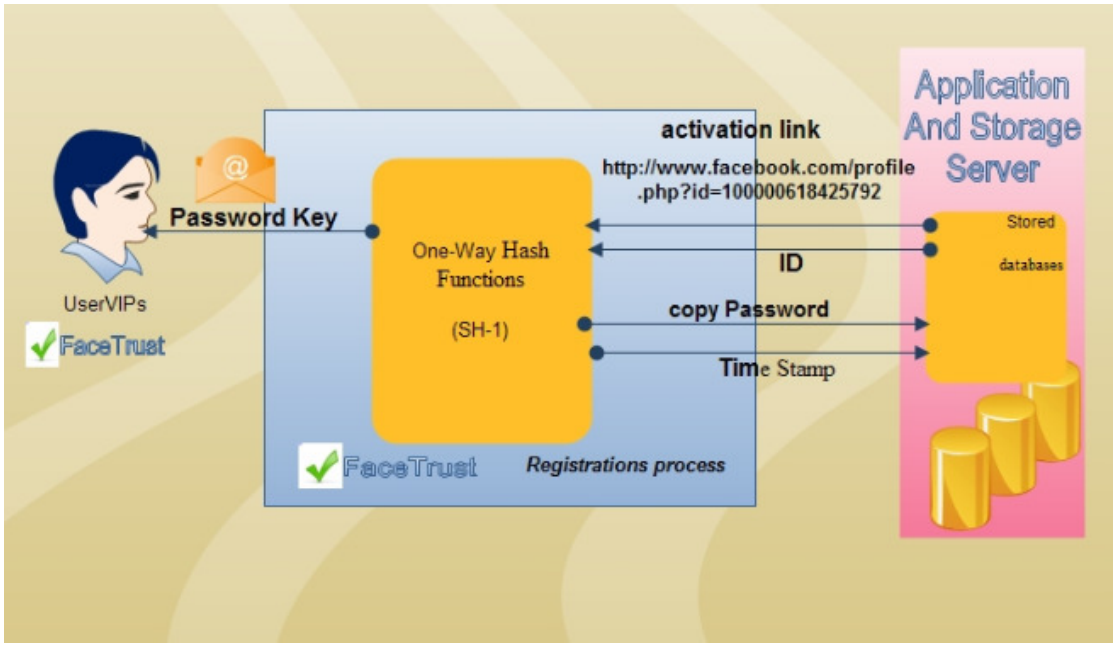


Figure 3-10: Process Generator Key

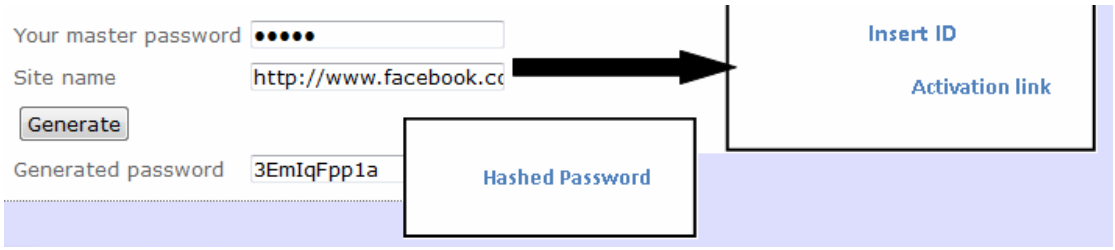


Figure 3-11: Hashed Password by SHA-1

II. Trust Logo process

This section 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 through the Photoshop programming. Figure 3-12 shows the process of producing trust logos.

Figure 3-12: Image processing using watermarking to produce trust logo

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, 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.

3.3.3 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:

1 - 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.

2 - 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.

3- 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; Figure 3-13 shows the trust logo appears inside the VIPs image.

Figure 3-13: The trust logo inside the image of VIPs page

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.

Chapter Four

Analysis of the Architecture and Case Study

Chapter Four
Analysis of the Architecture and Case Study

4.1 Overview

This chapter addresses the analysis of the FaseTrust through using case study.

The FaceTrust application is working to build a safe environment on Facebook that provides services for VIP users by displaying a trust logo above the origin page image to reduce the risk of privacy violation and threats that faces the Facebook pages security.

So that the analysis and diagnosis situations of the architecture used the case study by identifying the problems and challenges within a FaceTrust, as well as developing a set of problems and challenges which face the VIP users and fans who use FaceTrust, in addition to the representation of a scenario using a pictures and illustrations, hance the processing of all problems and challenges to get the appropriate solutions in order to make correct decisions.

This study of Facetrust application will be restricted to solving the suggested problems and analysis of several characteristics of performance and security, so as to explain the appropriate method to solve the problem and how to proceed in order to access an effective architecture.

The Facetrust architecture will be analyzed to achieve a secured system to provide trust to VIP pages without problems, using a case study which includes a number of expected problems that face the architecture, VIPs and fans, so as to put a scenario of major operations to activate a service trust on VIPs pages, to benefit from the case study used in the discussion.

4.2 Case Study

The FaceTrst application is a third party linked with Facebook to improve privacy performance and find the problem solution for the fake pages by giving trust to VIPs pages, in order to become a distinctive and unique among easy to find by fans and friends, through verification and make sure the identity VIPs by getting personal information from the VIPs website. Therefore, the logo appears inside the image profile, so that it becomes a badge of the VIP pages to reduce the fake pages exploiting names and images for the dissemination of lies and distortion. Therefore, the FaceTrust application creates a mechanism to verify the VIP identities by the computerized authentication from personal information already gathered from the URL, as a result the trust logo will appear inside the page image and that is easy to recognized by fans.

The FaceTrust provides important services to Facebook users, in order to increase the trust and privacy in dealing with them, including:

1 - Give the trust logo to VIP pages that appear in profile image.

2 - Attracting fans to the VIP pages trusted.

3 - Reduce the number of fake pages.

4 - Give a ranking of the fans number that joined to VIP pages participating in the FaceTrust.

In the figure 4-1 the home page FaceTrust application, this page is located within the Facebook environment and adds some changes to contribute and provide the service required. The home page contains a number of options are:

1 Register in the service.

2 List VIPs registered in the FaceTrust service.

3 Ranking the fans joined to VIP pages.

4 Help center and contacts us.

Figure 4-1: FaceTrust Application Homepage

The case study will consider a set of problems and events through the analysis and diagnosis situations in order to process and find appropriate solutions, so there are a detailed analysis and representation in the form of illustrations. These problems have been divided into two parts. They are:

1 - Problems facing the VIP users who use Facebook, which urges the usage of FaceTrust and finds a safe environment.

2- Challenges and restrictions that may face the FaceTrust application.

4.2.1 Problem and solution

Problem1:

This section will display the problems that users worry in dealing with their account on Facebook, so that they increase the feeling of fear and about mistrust for several reasons:

1 - Easy create account on Facebook, using e-mail as a condition for participation.

2 - There is no verification mechanism to ensure the real identity of owner page.

3 - There are no strict rules imposed on the violators and vandals.

4 – The Facebook principle is the participation in the service for free, thus does not seek profit.

5 - Some user's behavior that exploiting the VIPs names and images for the dissemination of lies and defamation, which leads to concern users.

The figure 4-2 shows the Facebook signup page, so that view the main options of the services, but there is no option to make sure the identity account.

Figure 4-2: Facebook Signup Page

Figure 4-3 shows an example of a large number of fake pages, which exploit the image and the king of the Hashemite Kingdom of Jordan name, King Abdullah II, so that is difficult to identify and make sure the VIP pages and lack of a hallmark indicator to the real page. Accordingly, the current Facebook there is no effective mechanism to reduce the fake pages problems.

Figure 4-3: Search Results for a Facebook page

Solution:

The solution to VIP pages is to participate in the Facetrust application, which works to make the logo appear inside the profile image, so that it recognizes the fans to favorite page through the prior knowledge that a Facebook application gives trust and verifies the identity the page. Also it requires the participant in the service to have an account in Facebook and web site.

The verification of personal information through the computerized mechanism authenticates this information stored in content URL.

So that the possibility distinguishes Facebook's pages, especially VIPs page, and thus is distinguished fake pages from the real pages easily through appear logo inside image, note that subscription with the Facetrust service is a free, so anyone can join with the service and get the trust logo, but the service require a personal website that have all your information.

The figure 4-4 shows the possibility of distinguishing the VIP pages that contain the trust logo, to make it easy to identify the fake pages that exploit the VIP names and photos, in the example of the Islamic personality, Dr. Amr Khaled.

Figure 4-4: Example of Fake Pages for (Dr. Amr Khaled)

- **Problem2:**

The ranking of facebook page participants and fans is an important thing, thus becomes to join large numbers of fans to VIP pages on Facebook utilized for media issues, also another problem appears with fans that increasing the concerning in dealing with the favorite pages and inability to validate this page. Consequently, the fans number is considered as a famous measurement for Facebook pages and ability to broadcasting media. Also there is no real method to get a realistic ranking for fans.

Solution:

The FaceTrust application provides a service to distinguish a VIP pages and the possibility of recognized upon the fans. The FaceTrust also provides ranking a service, which can be through knowing the best pages on Facebook that contain a large number of fans; The figure 4-5 shows the ranking page into the FaceTrust application.

Figure 4-5: FaceTrust Ranking Application

4.2.2 Challenges and Restrictions

There are some challenges that may face FaceTrust application, thus affecting the operations and constitute a threat to the Facebook users, which leads to put the measures security and preventive with an expectation weak points that affect the application performance to provide a service for the trust VIP pages.

So studying all the challenge cases and problems that may threaten architecture and exposure the risk is a basic purpose and the role of the Facetrust to protect the pages from risks that result in the illegal use, as well as to find solutions and procedures to raise the trust level; The purpose of the analysis is knowledge feasibility by adding a third party on Facebook to improve performance or solve problems related to users.

In addition to the restrictions in using of FaceTrust application to ensure preventing the Facebook cheating to obtaining the trust service, the study expected scenario for the operations conduct in order to get an easy and brief procedure, the result restrictions on access to control processes within an application to increase the security and trust.

4.2.2.1 Challenges facing the use URL

The URL of the main topics is to document information for VIPs, in order to access the basic information and make sure real identity, considering the URL as the primary key to get the service's trust, so that it is a clear challenge to the FaceTrust application, to avoid the leading to service destruction and reduce these problems have been to study all challenges and develop solutions.

These challenges are:

Challenges1:

The challenge is to try vandals to enter the right URL for the VIPs is unwanted to participate in the FaceTrust application or try to suspend service for VIPs enter their URL. And also FaceTrust is working on activating the trust service on the VIP pages using the URL for a single account on Facebook, any attempt to enter a URL by unauthorized would lead to suspending service.

Solution:

The solution for this problem is using verification and activation mechanism on FaceTrust so as to be sure and verify the identity of an applicant, through sending a password to e-mail is located within a URL. In this process it is difficult to access the password for vandals exploited to affect the trust service, so enter a URL for the FaceTrust is starting the process to get service by the applicant who results from reservation service for website. As a result of this method it will start a time stamp in the FaceTrust application which a specific time period when it begins to send password and ending after 48 hours. So the absence the activation in time will result in automatically to delete a subscription service FaceTrust.

As a result, the FaceTrust establishes an effective mechanism to control and confirm the arrival service to applicants by time stamp, which leads to increasing the VIPs confidence and fans, the FaceTrust ability of dealing with challenges.

Challenges 2:

The most important challenge is to follow the vandals clever tactics for the FaceTrust services by following the correct procedures, accordingly work to establish a correct website and recorded formally in the web host hence the recorded a fake information about VIP, in order to exploit how to get the FaceTrust service through

the URL. vandals for whom the prerequisite to get service FaceTrust is having knowledge that URL is effective, which leads to participation in the service and gets the trust logo within the fake page on Facebook but actually joins in the service FaceTrust. The result is used to mislead the fans and discredit VIPs. However, there is no effective mechanism to control, so this process constitutes a weak point in the architecture but can reduce the downsides.

Solution:

To reduce the risk of the correct use of URL to get the service trust logo within a fake page on Facebook, so that it develops mechanisms to reduce threats and the problems effects, as follows:-

1- The matching process between personal information within the URL with the information stored in Facebook profile.
2- Modifying settings of the Facebook page to prevent changing the personal information and contents manipulates.
3- FaceTrust's comparing continuously the information in profile and information obtained from a URL.
4- Using the service (Report/Block) to allow the fans of the page to monitor page behavior and judge the truth of the page, so if noticing any abuse or distortion is notified by FaceTrust, if repeated, the messages reporting abuse the page will be blocked by the FaceTrust service automatically.

Furthermore, the FaceTrust like any third party within the social networking, deals with users by principle trust and contract based on good intentions, besides it is difficult to determine the intentions and direction of users.

4.2.2.2 Challenges facing the trust logo

The challenges facing trust logo service provided to VIP pages, the possibility of theft the trust logo then put it on the image and used into a fake page, consequently, that misleads the fans by containing the logo image that confirms the participation a fake page in the service FaceTrust. So that they use the Photoshop to steal the logos to appear like the real logo, which leads to increase of the risk that faces the VIPs and reduces confidence in using the FaceTrust application. Nevertheless, the architecture has developed solutions to reduce the effects of this problem.

Solution:

The architecture working to reduce the risk fraud and theft the trust logo to be used illegally, through directing fans to know the VIP pages which are participating in the service FaceTrust, by following these steps:

1- Select the VIPs list which is registered in the Facetrust Home Page.

2- Search by the name by introducing the search box.

So the participant VIPs within the FaceTrust service will be viewed in the search results as a link that is connected to the VIP page on Facebook, in the figure 4-5 shows the search results, besides the use as a guide to know the VIP pages having a trust. Note that using watermarking in architecture just to generate the logo but does not use to discover a fake logo.

Figure 4-6: Search results in Facetrust Application

4.2.2.3 Challenges facing the lost password

The other challenge facing the FaceTrust is the password loss sent to the applicant, so that this password is used to activate service and to get activation link. Consequently, without the password the page does not have a service and also because the FaceTrust application gives the service trust to one account on the Facebook, it is difficult to send another password to same account and suspend subscription again to a website previously registered.

Solution:

The architecture found the solution for the lost password through using a time stamp mechanism, thus verifying the loss password by the applicant and password service revocation. If it exceeds the period specified it begins time stamp in the FaceTrust application which a waits that specific time to send the password and ending after 48 hours.

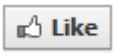
Accordingly, the applicant who lost password cannot participate during the period specified by the time stamp. Therefore, the FaceTrust application automatically unsubscribed, and possibility tried again to register and make sure to follow the correct procedures for participation.

4.2.3 Scenario

Therefore, it is necessary that the VIPs should know the procedures and tasks that enabled them to participate in the FaceTrust service and get them without complexities in procedures. This section shows the scenario how to subscribe for the FaceTrust by the graphic forms, so that it uses like the registration guide to show the correct procedures completely register, by following some steps in order to register in FaceTrust application:

1 - Login VIP to their account in Facebook.

Figure 4-7: Facebok Login

2 - Visiting a FaceTrust application by the link or click the icon application in the advertisement's bar, then participate in the FaceTrust page by clicking on 

.

Figure 4-8: FaceTrust application link in advertisements bar

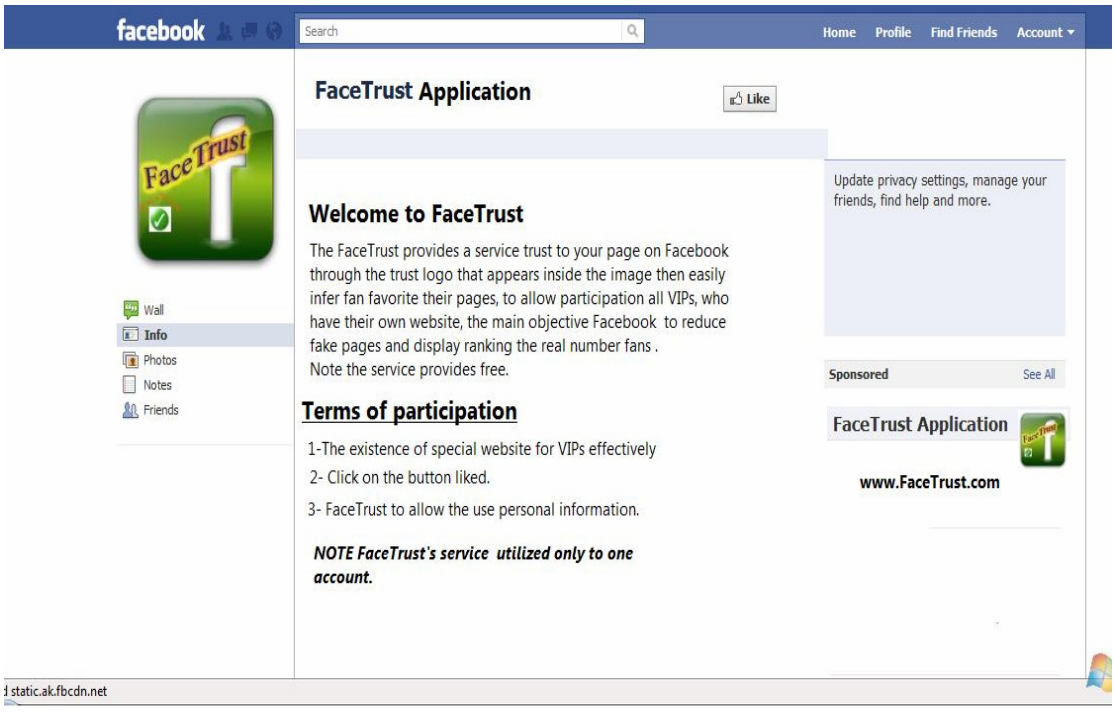


Figure 4-9: FaceTrust Application page

3 – In the home page of the FaceTrust application contains a number of options, and a guidance notes that display the advantages and conditions registration in the trust service, subsequently click on the option to register in the service.

Figure 4-10: FaceTrust Home page

4 - Display window that requests permissions in order to view personal information and control settings page.

Figure 4-11: Permission request window

5 - Registration window appears through which the VIPs enter their own URL in a box titled by (enter website address).

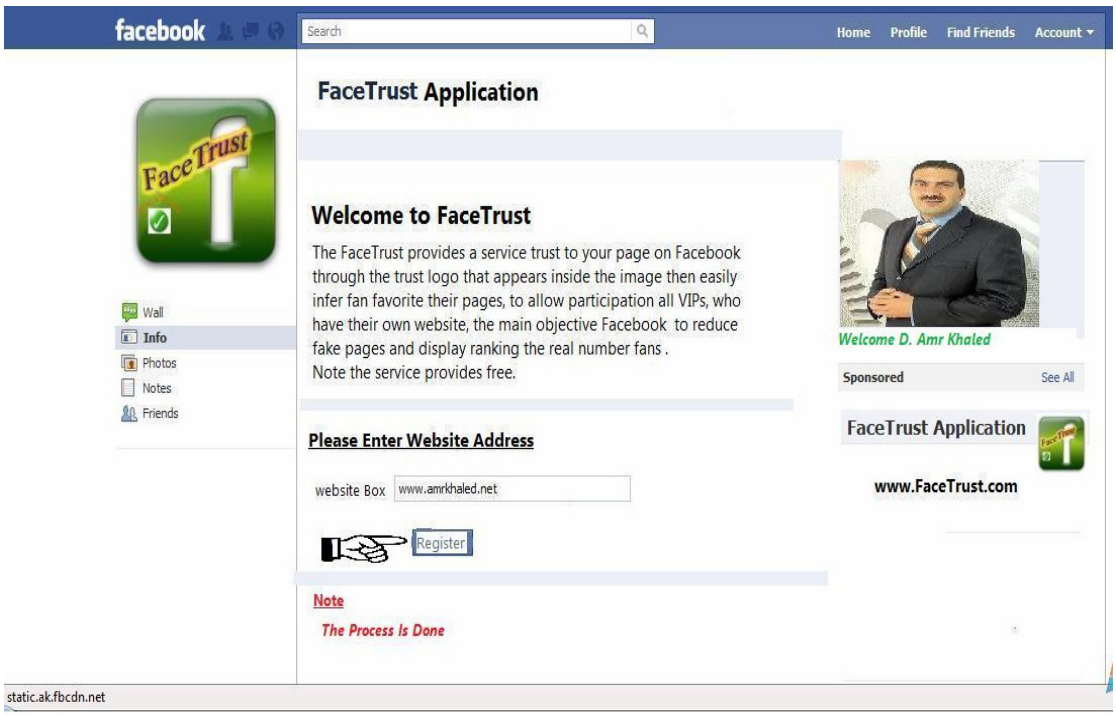


Figure 4-12: Entering the website address For registration

6 - The FaceTrust starting needs a procedure of generation a password in order to complete recording the result; after that the VIP enters his own website address successfully the password has been sent to the VIP email found content the URL. The figure 4-13 displays the password sent to the e- mail**.**

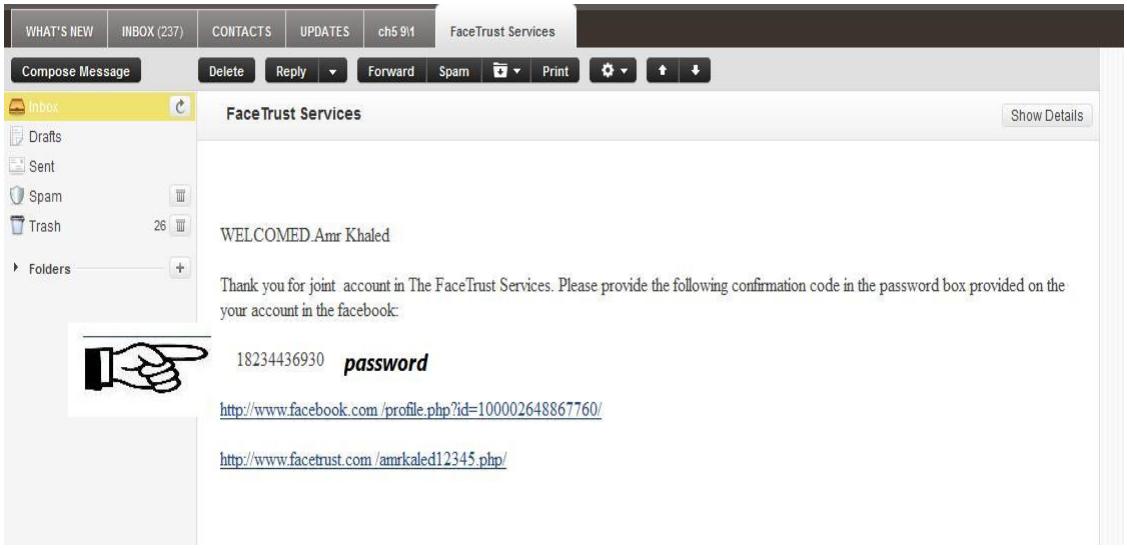


Figure 4-13: Random password sent by password generation

From FaceTrust applcation

7 - The VIP login again into his Facebook account and visits the FaceTrust home page application afterwards selects the option to register the service, then enter the valid password in a box (enter the password) and click on the register button.

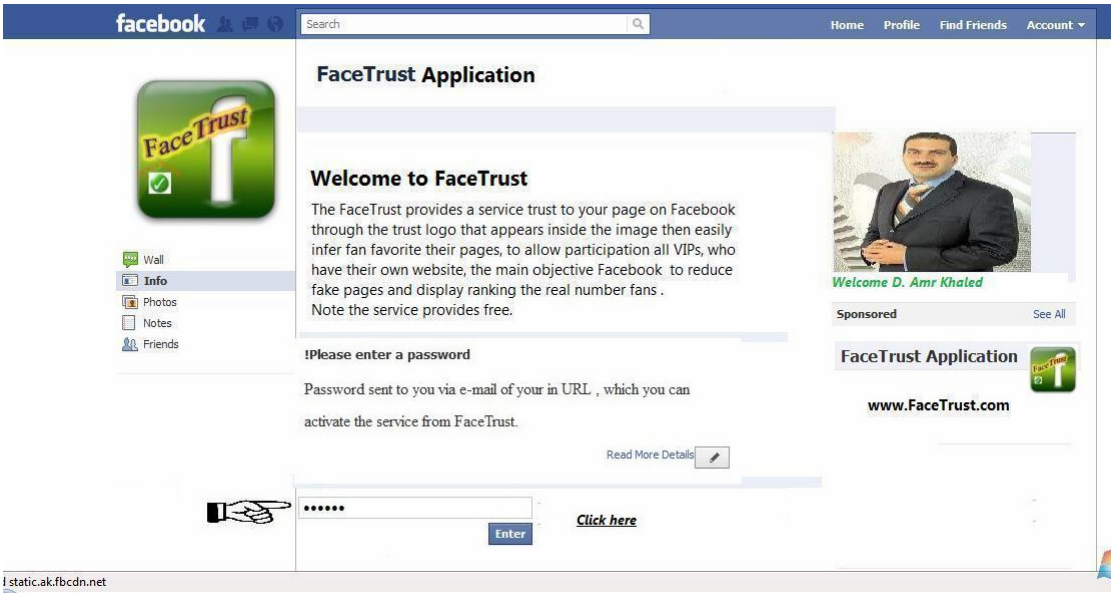


Figure 4-14: Entering the password that sent to user Mail

8- After the password has been verified the service activation link will be displayed; and then by clicking on the link the service trust starts automatically after refresh the page, which leads to the view the modifications on setting page.

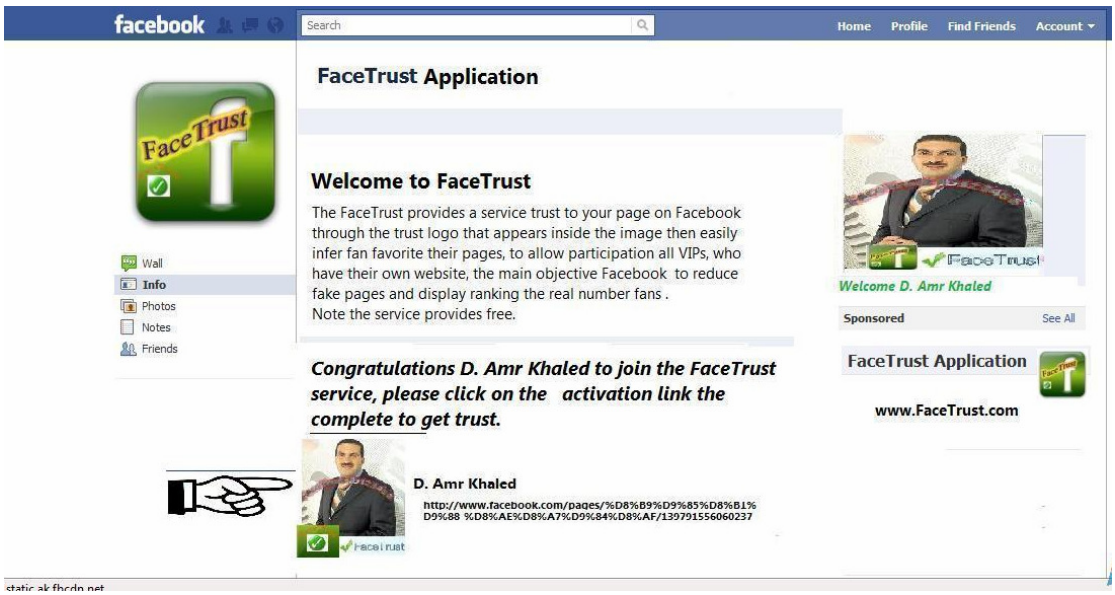


Figure 4-15: FaceTrust page after validate the password

9 - Example of a VIP page after the trust logo appeared inside the page image and FaceTrust icon in the toolbar Facebook. Figure 4-16 shows an example of a participated page in the trust service.

Figure 4-16: An example of a participated page in the trust service

4.3 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.

They discuss 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 figure 4-16 shows an example of the easy acknowledge a VIPs page via the trust logo among the fake pages, but the absence of this trust service in VIP pages will increase the problem's violation of privacy and fake pages. Therefore, that the Facebook in its current situation there is no effective solution to reduce the risk of fake pages.

Figure 4-17: Example how the trusted page viewed in the results

After the case study of the FaceTrus application architecture through comprehensive analysis to the anticipated problems and challenges that may face the application or users, the outcome to find effective solutions in order to reduce the incidence problems and risks that possibly will be possible in the future for architecture.

Discussion of the architecture with other researches achieved the same objective where there is no study at this time that provided a solution to reduce fake pages or give the trust logo. Thus it called the new architecture to give trust and privacy, but benefit from the studies related to adding a third party for social networking to improve the performance or a solution to problems that may appear in the architecture such as encryption or increasing privacy.

This is besides avoiding the problems posed by the previous studies in order to find architecture able to deal with the social networks effectively.

So that the benefits from research (The FaceCloak) used for that similarity the principle work with FaceTrust and the comparison between them into several directions. Thus, the FaceCloak does not include the revocation key that is used about the lack of key. As a result this leads to an absence trust in the process encryption information; The FaceTrust solves the problem of the lack of keys by mechanism time stamp, which is key revocation for lost passwords.

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.

Chapter Five

Conclusion & Future Works

Chapter Five
Conclusion &Future Works

5.1 Overview

This chapter presents the main conclusions of this thesis and suggestions for areas in the fields of trust & privacy on the social network that need further research and improvement.

5.2 Conclusion

All types of social networks such as (LinkedIn, Facebook, twitter and MySpace) became famous and interesting for internet users in recent years', in order to create an environment for communication among users and to find effective relationships between millions of users having shared interests without restrictions or oversight, to become a characteristic this time. It also is an important role in the intervention policies in countries. Consequently, a new path was created for the use of (actors, singers, political personalities, news sites, television sites, voluntary societies and other) in dealing with fans via pages on SNS; this group is called VIPs because of their special attention.

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.

The major challenge that will face the new architecture is easier to steal the trust logo by vandals, so that there is a need for finding an effective solution to reduce the risk through the guidance of users to visit the FaceTrust application page on Facebook then search for a VIPs name who joins the service; then as a result a link will be viewed, which redirects the users to the real page.

Finally, the presence of the new secure architecture that improves the Facebook trusting and finds an effective solution to the fake pages problem with threatens privacy, as well as its ability to repair the defects and problems that appear on the Facebook architecture; thus impacting positively on Facebook and increases the VIP activities and the number of participants on their pages. Besides FaceTrust is applied on all types social networks because of the similarity in the main functions and objectives plus exposure of the fake account problem and the lack of effective solution within their applications.

5.3 Future Works

There are many issues related to privacy and trusting on SNS, which require search in order to find a safe environment for users, as well as to find alternative solutions to defects and problems within social networking architecture by adding a third party. As a result, the existence of FaceTrust as a solution of the fake pages will decrease the risk and a threat vandal so that future studies to reduce risk potential to create an integrated system service that provides trust.

The new architecture can be a starting point research in various domains in order to improve the performance of the social networking and finding solutions with its problems. It is advised in the future to research in the following areas:

1- Implementation of a new architecture and activation within Facebook to provide trust service with the VIPs pages.
2- Find a solution about stealing the logo problem and illegal using by vandals through cooperation with Facebook to compare images that hold a logo with the rest images in order to suspend the fake accounts.
3- Activation of the FaceTrust to provide service for more than the account on Facebook rather than one account.
4- Using the FaceTrust application on the rest of social networks through the individual study as well as changing some features of the FaceTrust to suit all types of SNS.

So this study provides an important reference for researchers for helping them to build a security system and finding a third party to resolve problems related to social networking that appear with the passage of time; Finally it provides a reference to develop a third party in the future in order to make security services for social networking.

Reference

[1] AlpVision,(2011), In AlpVision SA, The Digital Watermarking, 09:32, July 15, 2011, (On-Line), from: http://www.alpvision.com/watermarking.html.

[2] Arab Spring. (2011, July 15). In Wikipedia, The Free Encyclopedia. Retrieved 23:21, July 16, 2011, (On-Line), availablehttp://en.wikipedia.org/w/index.php?title=Arab_Spring&oldid=439676886

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

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

[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. (2007). 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.

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

[8] E. Steel and G. A. Fowler, (2010) "Facebook inonline privacy breach; applications transmittingidentifying information," available: http://online.wsj.com/article/ SB10001424052702304772804575558484075236968.html.

[9] Facebook Query Language. (2011, April 21). In Wikipedia, The Free Encyclopedia. Retrieved 07:15, July 17, 2011, (On-Line), from http://en.wikipedia.org/w/index.php?title=Facebook_Query_Language&oldid=425195445

[10] GAHANNA,A., (2007). 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

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

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

[13] KELLY,D.,(2011). 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

[14] 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.

[15] Persits, P. , (2011),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.

[16] SHA-1. (2011, July 10). In Wikipedia, The Free Encyclopedia. Retrieved 07:55, July 17, 2011, from http://en.wikipedia.org/w/index.php?title=SHA-1&oldid=438682918

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

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

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

[20] V. Shah ,(2009), Fair Trade Awareness through Social Networking Mediums and an Insight into Collaborative Filtering , Report is submitted as part requirement for the *MEng* ,pp 18.

[21] 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

[22] Whois,(2011). 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***

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

[24] 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.