CHAPTER II

LITERATURE SURVEY AND PROBLEM FORMULATION

The literature studies are grouped into three categories namely technical, social and technical akin to social of SNS authentication. The research problem formulated from these studies is summarized. Appropriate references are cited as and when necessary in other chapters.

2.1 TECHNICAL SECURITY ISSUES IN SNS

Differences are aplenty between different security authentication techniques [Anand Sharma & Vibha Ojha – 2010] and therefore they need to be classified for comparative analyses. This is needed so that the advantages and disadvantages of different secure authentication methods can be highlighted for different application needs. This would also help researchers in improving and modifying authentication techniques. Literature has dealt with specific issues along with merits of several authentication techniques such as Brute Force attack, Dictionary attack, Surfing, Phishing, etc., of different authors.

The conventional password scheme, even though old, it is the most widely used [Mudassar Raza et. al. 2012]. The user enters his login and password when he starts using the system. Grant to use the system is permitted once the user provided login name and password matches in the database maintained by the system. Only registered authenticated users are permitted by this scheme. But this scheme is vulnerable to authentication attacks such as surfing, phishing, key loggers and Login Spoofing etc. Therefore it is essential to study the merits, demerits and issues of different attacking techniques. A similar but different technique is the use of authentication panel [Manabo Hirano and Tomohiro Umeda, 2012]. In this scheme, the user instead of pressing exact buttons for password, user is allowed to locate the passwords from a panel. This method is safe against Brute Force, Dictionary, Shoulderering and Video Recording attacks, those have different issues. These attacks would also be dealt with, in another Reformation Based Authentication, the passwords are shifted to new forms before storing them in databases in a dynamic manner. For verifications of such reformed passwords require
verification by using reform mapping [Safdar S, et. al. 2010]. Hawkers would be unaware of real passwords as per this method. There is another important and a novel technique, which uses a password over another password [Shahid M and Qadeer M A, 2009]. The user must remember two passwords and also the private key of the system. It is a highly secured system.

All possible combinations of password are applied to break password through Brute Force Attack [Fujita, K & Hirakawa, Y – 2008]. This attacking method is applied to generally crack encrypted passwords in the form of texts. In UNIX and early LINUX based systems, passwords are kept in separate files encrypted in the form of Hash. Message Digest algorithm Ver.5 (MD5) Hash form was used. Therefore, the attacker who uses Brute Force technique first converts all combinations of passwords into their MD5 form. The hash is then matched with the corresponding password of selected. But Brute Force method is more time consuming as searching a hash from all possibilities. This indicates providing hashes and checking user provided passwords might be less quicker and irritate particularly children users. Compared with Brute Force method, Dictionary attack is relatively faster [Arvind Narayanan & Vitaly Shmatikov, 2005]. Unlike the Brute Force method this method tries to match most occurring words of daily life of the dictionary, like names of birds or famous places etc. The Brute Force method on the other hand checks all possibilities, and hence takes more time. But dictionary attack has some limitations. For examples, non popular proper nouns are not present in dictionaries. In view of the above, hackers try to use ‘surfing’ as alternative technique to hack passwords. In one of these types of techniques, known as Shoulder surfing, the hacker tries to spy user’s movements to obtain his password. Different techniques adapted in this technique matters as the nature and age of password users and specification/usages of their passwords are sensitive [Huanyu Zhao Xiaolin Li 2007]. The attacker can obtain passwords by directly or indirectly be friendly with the users and try to spy on the passwords. On the other hand, hackers may try to trick users through e-mails, the technique known as phishing. This is an important technique to be studied, as children users might be vulnerable, as for example, similar looking site names like ‘yah0o.co.in’ may look like ‘hahoo.co.in’. The hacker then redirects the user to the original web site, after obtaining the passwords. Phishing control filters may not be fully operable and therefore not reliable [Fahad Ikram et. al – 2008]. When an attacker attacks, the authenticator (user) challenges the responses. For example, the attacker enters his name in the
first login connection. The device of the authenticate user challenges the attacker [Syverson et. al 1994]. The attacker then opens another login at the same time with the same name of the authenticate user and replies to the challenging device as challenge of previous connection. The attacker sends back the reply challenge and gets its authentication. This technique is also known as ‘Reply Attack’. This technique deploys a lot of interactive sessions. Certain attack techniques like spoofing is similar to phishing, but in certain aspects they are distinctly different. The use of key loggers is similar to spoofing attack. Key loggers are software used in recording every user action on the key board of his system. Installation of such software is trickily done by the hacker like physically doing it in user’s system or instructing the user to clique install icon [Baig & Mahmood 2007]. Therefore it is vulnerable to children, particularly. The key press recorded by the hacker’s software would send the data, later, to the hacker’s system.

Keystroke dynamics is another attacking technique, which records the speed of pressing and releasing keys on the keyboard. As it is a hardware and human related physical activity based, it is time consuming and may be unreliable sometimes [Haider, S A Abbas and Zaidi A. K, 2000], because it does not tell what the user has keyed but only how he had keyed. As the timing of pressing; time of releasing; time kept pressed the keys etc., matters, the processing becomes complex. With this fact, the password rejection rate is high and it can be effective in different mental conditions of the user. Even though recording the regular patterns of authorized user and reject un authorized users, since the process is complex and rejection rate may be large even for authorized but inexperienced users like children. A similar but different from key stroking is Graphical password technique. In this technique, software displays different graphical objects [Qurar-Ul-Ain Arshad, et. al., 2007], from which the authorized user must select set of objects at the first time. Users are then allowed to draw the selected objects using drawing tools such as stylus, laser pens etc. The system forms hierarchical grouping of drawing elements selected by user and records them in a database. Every time, the user’s authentication is tested on the drawing with recorded hierarchy. This technique avoids surfing attacks and is more safe. But verification is passed only if the user has properly drawn. Processing time is very high. Users like children even though might like to draw, but processing would be irritating. Bio metrics, other methods, are similar to this graphical technique. Recognition by this method is based on image processing [Varun Kacholia and Shashank Pandit, 2003]. The biological elements for
recording and verifying by this method include: Finger print, Face recognition, Signature verification, Speech recognition and Iris recognition etc. In its first process the selected items are recorded by the system in a database. As real and unique features are tested, this system is highly reliable and cannot be stolen. The problems with this technique are: difficulty in implementing and costly. Above all it takes more processing time and the hardware might yield to wear and tear. Young children users might find it difficult and time consuming in using this technique.

Password attacking techniques need to be known to users for applying these techniques for protection against such attacks [Mudassar Raza et. al. 2012]. Besides some techniques are related to stand alone systems and others are for online systems. Different techniques can be merged together to form a single and more secured password schemes. Password based key exchange algorithms based on Diffie-Hellman algorithm were tried out by many authors since its origin, This method was enhanced to overcome security flaws in that method [Hwang R J et. al. 2003]. A cryptanalysis was proposed on this enhanced algorithm [Kou-Min Cheng et. al. 2010], since the protocol was suffering from security threats like Backward Replay attack and offline password guessing attack. An important conclusion had been drawn by these researchers. It is concluded that users hardly find it to use long random strings as passwords. It is suggested to use natural language phrases instead of random long strings as passwords. It will be easy for the users (particularly minor users) to remember natural language phrases. But however there are limitations in building phrases out of natural language.

Signature based authentications without the use of hash function on Diffie-Hellman’s public keys has been proposed [Lein Harn & Lin Y, 2001, Lein Harn and Jian Ren, 2008]. This method did not apply modular arithmetic earlier. But without hash function on key exchange protocol was successfully demonstrated. Enhanced version of Lin’s protocol was proposed [Ren-Junn Hwang et. al. 2003]. In this enhancement the computation time was reduced using X OR operation, thereby increasing the efficiency. However, this technique still did suffer from Forgery and Denial of Service attacks [Hwang R J et. al. 2003]. But digital signature using one way hash function would provide message integration, better authentication and non repudiation [Tzong-Sun Wu, & Chien-Lung Hsu, 2002]. But the design needs to be varied according to the purpose for which it has been proposed. Since Diffie-Hellman key agreement protocol is
vulnerable to man in the middle attack, Data origin authentication, proof of data integrity, proof of non repudiation, digital signature could be used. In addition, station to station protocol could be proposed as a remedial measure. An enhanced and secured key agreement protocol for exchanging multiple session keys for authenticating potential attacks was proposed [Siva Prasad M. V, et. al. 2009].

A comparative study on different algorithms of key managements for security has been documented [Sandro Rafaeli & David Hutchison 2003]. The algorithms dealt with both centralized as well as decentralized and distributed key management protocols were discussed. The merits and demerits of centralization and decentralizations were debated. Procedures for new member joining in a group and the protocol for key management in such situations were discussed [Renuka A & Shet K C 2009]. A hash tree based group key management protocol for such a situation has been documented. Distribution of keys between cluster heads has been proposed. Study on ad hoc network using simulation was performed.

A comparative study and performance analysis on common biometric techniques was presented [Parvinder S. S et. al, 2009]. Biometrics refer to recognition of physiological and/or behavioral characteristics of individuals. This is done automatically using hardware and related software. It does not deal with possession of identity, but allows anyone to confirm or establish an individual’s identity. 1998-99 saw maximum sales of biometric products that could recognize fingerprints. Fingerprints are analyzed using friction ridges that cover the fingertips and classify patterns of minutiae, such as branches and end points of the ridges. It can also look at the pores in the skin of the ridges.

2.2 SOCIAL ISSUES IN SNS

About 15 million teens in the U.S. were SNS users as of 2008 and about two million children of 3 years to 11 years of age had used SNS. 65% of the SNS children users have their profiles in the SNS [SNS McAfee, Inc. 2012]. These sites are like virtual club houses. Once a child becomes a member and create a profile, it can interact and connect with family and friends via online activities like chat, email, photos, events and status updates. These sites are popular to
children, as they can Communicate with friends and family; Meet new people; Reconnect with old buddies.

Share messages, videos, and photos; Plan their social life; Participate in a group or cause that interests them; and Play online games with other members. Thus online networking is more popular than e-mails for children. But problem with SNS for children especially is ‘too much information’. If the children reveal too much about their personal information, it could lead to problems. Some of the problems faced by children are:

**Flaming**: Online fights sent via email or instant message with angry or vulgar language;

**Harassment**: Repeatedly sending nasty, mean, insulting messages;

**Denigration**: “Disusing” someone online by sending or posting gossip or rumors about a Person to damage his or her reputation or friendships;

**Impersonation**: Pretending to be someone else and sending or posting material to damage their reputation;

**Pranking**: Tricking someone into revealing secrets or embarrassing information and then sharing it online.

Most general–purpose sites despite economic costs, social concerns, and technical issues, opt to restrict underage access through their Terms of Service [Danah Boyd et. al. 2011]. In spite of such restrictions, research suggests that millions of underage users circumvent this rule and sign up for accounts on Face book. There is strong evidence of parental concern about children’s online activity. This raises questions of whether or not parents understand Terms of Service restrictions for children. How they view children’s practices of circumventing age restrictions, and how they feel about children’s access being regulated. Since SNSs allow children to connect with their peers, classmates, and family members for educational, social, or familial reasons, parents knowingly allow their children to lie and get entry into SNSs. It is suggested that SNS service providers should present children with child-appropriate experiences and information designed to enhance safety, provide better privacy protections and encourage parent-child discussions of online safety. Age verification of users is a derivative of identity verification, while identity verification is done in SNS hundreds of thousands of time a day [John Dancu,
It is essential because it should be known who the SNS user for age verification is. A higher level of verification is actually knowledge based authentication. This is done for the following goals with respect to children users of SNS:

- To limit harmful contact between adults and children;
- To limit harmful contact between children;
- To prevent children from accessing inappropriate contents within SNS;
- To prevent children from creating inappropriate contents within SNS;
- To prevent children from accessing particular sites without parent consent;
- To prevent harassment, unwanted solicitation, and bullying of children of SNS.

When age of users of SNS is verified, then it will be possible to identify adult members to prevent harmful contact between adults and children because it separates the users and allows SNS to provide additional security measures where needed. Besides, it will prevent children to access inappropriate content within adult community. For example users of ‘MySpace’ of age over 18, cannot browse for users of age under 18 and vice versa.

There are many unanswered questions as to whether or not US Children’s Online Privacy Prevention Act [Boyd D et al [2011] has been effective. Particularly to what extent the parents of the minor users of SNS have understood age limitations in using SNSs. Besides, will SNSs be useful to their children? There is a high extent of US children lying about their age to gain access to sites that forbid them. Whether parents are unaware or agnostics about such restrictions?

Social Networking sites in India witness a high usage from women between the ages of 15 – 24 years [ViziSense 2010]. Different education profiles make a significant impact on social networking in India. There was a variation recorded over the usage patterns across the geography of India. Online usage is skewed in the ratio of 61% in favour of South Indian women, however, when it comes to social networking, their counterparts in North India are way more active. In fact, it was seen that out of the total unique users of social networking, 55% belong to North India and 45% belong to South India. Students show high activity on search and music sites with a peak in usage between 3:00 p.m. to 4:00 p.m. Questions on persona for
fallback authentication were tried out [Ariel Rabkin 2008]. The study was carried out using social survey. Weakness of personalized questions was identified. Answers to personalized questions need to be truly private to the user and therefore cannot be accessible to public. The protocol suggested on Diffie-Hellman algorithm’s enhancement to overcome security flaws [Hwang R J et. al. 2003] still might suffer that an intruder could share some session keys with others by getting an old message from a legitimate user [Chou-Chan Yang et. al. 2005]. To overcome this, the user’s secret key, that could be social in nature, was proposed to calculate the signature.

As preferred interests of SNS users are different, forums within SNS have gained popularity. Personal data of these users are generally obtained and preserved by SNS service providers. It is therefore risky, as disclosures to digital friends may lead to privacy and its security risks [Giles Hogben - 2007]. When children, particularly adolescents use these sites, security to their personal information become vulnerable and risks caused by chatting with friends become more. [Boyd D et al [2011] have brought out social survey results on children’s online privacy. Even though usability is extremely important for children, security should never be compromised in special children’s forums of SNS. The usability issues include cumbersome login procedures, confusing terminologies, inadequate feedbacks, error messages and improper links [Doug Fox and Shiva Naidu - 2009].

2.3 SOCIAL AKIN TO TECHNICAL ISSUES

A history of SNS with time line, the step by step evolution of SNS has been documented [Anchises M G de Paula, 2010]. The usage of SNS could be prolonged if adjustments and improvements existed in both technical as well as social to meet the user needs. Restricted forums within SNS should specify the classifications and features along with limitations. SNS is organized by its user interests. While the features of SNS are similar, various applications of it make the users feel difficult to use the system, as the contents are constituted based on its users’ interest and cultural differences [Doug Fox and Shiva Naidu, 2009]. 70% of Consumer privacy survey respondents did not like the unrestricted use of their medical data for research purpose [Helen Giggins and Ljiljana Brankovic 2008]. 76% of people believe that control on their
personal data and privacy is lost. 96% of the respondents wouldn’t like the secondary usage of their personal data delivered by the service provider, who has retained and maintaining the information. The major weakness of the internet is its lack of possession of well designed and highly usable infrastructure for reliable and privacy preserving authentication [Dirk van Rooy & Jacques Bus, 2010]. Certain factors have direct impact on the strength of passwords. In that case, password based security model in two phases namely adapting an Attack simulation model and Evaluation based on applying such models could be used to arrive at the factors for specific applications [Kuzma, Joanne 2011]. 30 global network sites had been analyzed for the levels of authentication have been studied and reported. From information security point of view, Social engineering refers to psychological manipulation of people into performing actions or divulging confidential information. Password based risk including social engineering attacks have been reported [Catherine S W et. al. 2010] and user perceptions of security along with usability and convenience in using SNS have been studied. One time token generation mechanism and three methods of it had been tried out and results evaluated based on efficiency and satisfaction in terms of usability through social survey were reported. It is argued that the steps for calculating one time token generation would increase computational time. Therefore this might decrease the usability. US Lawmakers, according to Children’s Online Privacy Protection Act 1998 (COPPA), intended that, by requiring SNS Service providing companies to inform parents of children users, their data-collection practices and obtain permission for uses of their children’s data. COPPA would provide parents with better tools to protect their children in an online era [Boyd D et al - 2011]. Even though most of the outcomes of COPPA are positive, it is conceded that, in response to COPPA, online industries generally have neither innovated nor emphasized mechanisms for obtaining verifiable parental consents. The US Federal Trade Commission, 2006 [Boyd D et al - 2011], received five comments relating to underage users. One of the comments quotes “Web sites follow Commission staff guidance and request age information in a neutral manner, and then set session cookies to prevent children from later changing their age”. But at the same time there is no way to prevent certain children from falsifying their age.

Traditional security mechanisms will not guarantee an individual’s privacy [Helen Giggins and Ljiljana Brankovic, 2008]. There are key issues in systems based on ‘Data Warehouse’ that must be taken note of. Sensitive information on individual’s records (such as

17
children users) in the data warehouse is not disclosed by answering queries. But higher levels of security (privacy) imply a lower usability. The real problem is how to find the best balance between these conflicting goals. An analysis of security in SNS has been made [Amos O Olagunju 2008]. The concept of Chinese remainder theorem on cryptography has been explained. The computational strength of the Chinese remainder theorem has been stressed. The features of social networkable users have been documented.

Non restricted users in SNS can quickly share photos or videos or communicate to connect via another SNS. This is true in restricted user forums of SNS too. Because of this nature of usability, ‘usability’ apart from ‘security’ plays an important role in restricted forums of SNS. Usability was a significant reason for not returning to use of SNS by many users [Doug Fox and Shiva Naidu, 2009]. The term ‘usability’ includes cumbersome login procedures, confusing terminologies, inadequate feedbacks, error messages and improper links. Therefore creation of private and restricted user forums within SNS, where protection is guaranteed of individual personal information, is gaining popularity.

Deniable authentication is a method that executes authentication verification between participants known to each other and they themselves are confident in the authenticity process. Once the event is over, third party cannot be known about the authenticity. This technique had been tried out with biometrics [Muhammad Khurram Khan, 2013]. Biometric when used along with deniable authentication protocol had been demonstrated to protect impersonation as well as coercion attacks. In the proposed scheme, the deniable authentication is introduced once a sender is successfully verified by his biometric. The combination of biometric and deniable authentication is technical akin to social. The crux of biometric security problem lies with its strength [Parvinder S. S et. al, 2009]. There are two sides of every coin and biometric system has no exception. One is the robust secured side and the demerit side is due to bugs, blunders, and complacency. Biometrics are sensitive to environmental conditions, like noise, dirt, vibration, and unreliable lighting conditions, even though advantages exist in the form of alarms, seals and tamper sensing.
A fingerprint biometric was fed with a fake fingerprint on the sensor, for an experiment [Anil K, Jain & Umut Uludag, 2003]. In another experiment, a digitally stored biometric data was fed. In the third experiment, instead of actual values generated by the biometric system, a failed system was forced to produce feature values chosen by the attacker. In the fourth experiment, a set of synthetic features were replaced for a features extracted from a sensor. In the fifth attack, the matcher component could be attacked to produce high or low matching scores, regardless of the input feature set. Such types are capable to decrease the credibility of a biometric system. For the sake of investigating wide spread utilization of biometric security techniques, these experiments were planned. In all these experiments different types of techniques such as encryption, watermarking, and steganography were planed. Factors of decoding accuracy and matching performance were highlighted from the experiments. It was concluded that the security and integrity of the biometric data itself are important issues. Watermarking, Steganography and Encryption are possible techniques to secure biometric data.

2.4 SUMMARY FOR RESEARCH PROBLEM FORMULATION

The most important findings as reported by the literature have been grouped and summarized for the purpose of problem formulation. This summary is presented in Table 2.1.

Table 2.1. Findings from literature that has led to formulation of research problem.

<table>
<thead>
<tr>
<th>S.No</th>
<th>Important Findings</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security authentication techniques need to be classified according to their performances for comparisons. It is essential to study the merits, demerits and issues of different attacking techniques</td>
<td>Anand Sharma &amp; Vibha Ojha – 2010. Manaboo Hirano and Tomohiro Umeda, 2012</td>
</tr>
</tbody>
</table>
The literature study evidences that most of the research objectives and research questions stated in Chapter I have been vindicated. Table 2.1 that has consolidated important issues and the edifice that have been extracted has supported this. From these analyses and appraisal of the literature surveyed, the research title namely “SECURITY AKIN TO USABILITY IN MINOR USER GROUPS OF SOCIAL NETWORK SITES” has emerged.

| 3 | Some techniques are related to stand alone systems and others are for online systems. Different techniques can be merged together to form a single and more secured password schemes. Password based key exchange algorithms based on Diffie-Hellman algorithm was tried out by many authors since its origin. This method was enhanced to overcome security flaws in that method. | Mudassar Raza et. al. 2012. Hwang R J et. al. 2003 |
| 4 | Problem with SNS for children, particularly is ‘too much information’. If the children reveal too much about their personal information, it could lead to problems. The protocol suggested on Diffie-Hellman algorithm’s enhancement to overcome security flaws still might suffer that an intruder could share some session keys with others by getting an old message from a legitimate user. | Danah Boyd et. al. 2011. Hwang R J et. al. 2003. Chou-Chan Yang et. al. 2005. |
| 5 | 76% of people believe that control on their personal data and privacy is lost. 96% of the respondents wouldn’t like the secondary usage of their personal data delivered by the service provider, who has retained and maintaining the information. Because of this nature of usability, ‘usability’ apart from ‘security’ plays an important role in restricted forums of SNS. Usability was a significant reason for not returning to use of SNS by many users | Helen Giggins and Ljiljana Brankovic 2008. Doug Fox and Shiva Naidu, 2009. |