Prevention Of Online Identity Theft Using Bio-Threshold Scheme

E.S. Mughele
Department of Science & Technology
Computer Science Option
Delta State School Of Marine Technology
Burutu, Nigeria
Prettysophy77@yahoo.com

ABSTRACT
The tremendous opportunity to learn, share, connect, shop, and bank due services such as World Wide Web, email, E-commerce, and so on, provided by the internet have become very important technological advancement for both individual and businesses. The misuse of person’s data for impersonation and abuse of banking/financial services facilities is a growing concern in developed as well as developing societies. This paper hereby, proposes Biometrics (Fingerprint) and threshold cryptography as techniques for prevention of identity theft.

Keywords: Identity theft, Identity fraud, Impersonation, Biometrics, Threshold cryptography

1. INTRODUCTION

Services such as World Wide Web, email, E-commerce, and so on, provided by the internet have become very important technological advancement for both individual and businesses because it offers tremendous opportunities to learn, share, connect, shop, and bank. Yet, emphatic measures have not been taken to ensure security of user’s information. According to Information Commissioner RS [6], the fastest developing type of criminal activity in the last decade is known to be identity theft. The terms “identity theft” and “identity fraud” have come to be used interchangeably in popular usage, even though the two are different from a legal point of view (Newman and McNally, 2005). Identity theft is defined as the “misuse of another person’s identity, such as name, social security number (SSN), driver’s license, credit card numbers, and bank account numbers” [3] while Identity fraud occurs when a false identity or someone else’s identity details are used to support unlawful activity, or when someone avoids obligation/liability by falsely claiming that he/she was the victim of identity fraud (FPEG Report, 2007).

According to the Identity Theft Resource Center, identity theft is sub-divided into four categories [11]:

- **Financial identity theft**: This is using another’s identity to obtain goods and services.
- **Criminal identity theft**: This is posing as another when apprehended for a crime.
- **Identity cloning**: This is using another’s information to assume his or her identity in daily life.
- **Business/commercial identity theft**: This is using another’s business name to obtain credit.

CIPPIC [1]) opines that identity thieves tend to steal twelve types of private personal information such as; credit card numbers, CW2 numbers (the back of credit cards), credit reports, social Security (SSN) numbers, driver’s license numbers, ATM numbers, telephone calling cards, mortgage details, date of birth, passwords and PINs, home addresses and phone numbers. This misuse of person’s data for impersonation and abuse of banking/financial services facilities is a growing concern in developed as well as developing societies. The consequences of identity theft can be unforeseeable for the victim; because he can even become liable for acts he did not commit [6].

2.0 RELATED LITERATURES

2.1 Biometrics

Biometrics is automated method of recognizing a person based on a physiological or behavioral characteristic. It is considered a reliable solution for protecting the identity and the rights of individuals as it recognizes unique and immutable features [2][5]. The biometric approach is based on the fact that many characteristics of an individual are unique and hardly change over a lifetime [11]. Biometrics is used for two authentication methods:

- **Identification**: This involves establishing a person's identity based only on biometric measurements. The comparator matches the obtained biometric with the ones stored in the database bank using a 1:N matching algorithm for identification [7][8].
- **Verification**: It involves confirming or denying a person's claimed identity. A basic identity (e.g.
ID number) is accepted and a biometric template of the subject taken, is matched using a 1:1 matching algorithm to confirm the person’s identity.

Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information [7].

2.2 Threshold Cryptography
According to [2], the concepts of group oriented cryptography and threshold cryptosystems were developed by Frankel and Desmedt. Since then, there has been much work devoted to the topic such as Desmedt and Frankel, Pedersen, Gennaro et al. and many more [11][12].

Threshold cryptography is a branch of public key cryptography in general and multi-party computation in particular. Essentially, in a k-out-of-n threshold cryptosystem, denoted (k,n) where 1<k<=n, for the RSA function, the aim is to generate and then split the secret decryption/signing key into n different pieces, which are then distributed privately to n parties. This enables:

- Any k or more out of n total parties, when they come together, they can “reconstruct” the secret key a way which enables them to decrypt or sign a message. This should be done in a way that does not reveal the value of d and its shares to anyone in the scheme.
- Secondly, signing or decryption will be totally impossible in the circumstance where less than k parties are present.

However, the majority of these solutions are only for discrete logarithm based systems that has a direct application to the Elgamal encryption and decryption algorithm (Rahman et al., 2010).

2.3 Discrete Logarithms
Let $G = <g>$ be a group of prime order q, such that g is a generator of G. The discrete logarithm problem (DLP) means, for a random $y \in G$, compute $x \in Z_q$ such that $y = g^x$. The Diffie-Hellman problem (DHP) is to compute $g^{x_1x_2}$ from random $y_1 = g^{x_1}$ and $y_2 = g^{x_2}$. It is conjectured that there exist groups in which solving the DLP and DHP is hard, for example, the multiplicative subgroup $G \subseteq Z^*_p$ of order q, for some prime $p = mq+1$, where $|p|=1024$ and $lq|=160$ (recall the q is prime).

2.4 ElGamal Encryption
The ElGamal cryptosystem is based on the Diffie-Hellman problem. Key generation chooses a random secret key $x \in Z_q$ and computes the public key as $y = g^x$. The encryption of $m \in \{0,1\}^*$ under public key y is the tuple $(c_1,c_2) = (g^r, m^y) \in G \times \{0,1\}^*$. The decryption of a cipher text $(c_1,c_2)$ is $m = H(c_1^x) \Theta c_2$.

One can easily verify that $m = m$ because $c_1^x = g^x = g^{xy} = y^x$; and therefore, the argument to H is the same in encryption and decryption. The scheme is widely considered to be secure against passive adversaries.

2.5 Threshold ElGamal Encryption
The threshold ElGamal cryptosystem tolerates the passive corruption of t < n/2 parties. Let the secret key x is shared among $P_1,...,P_n$ using a polynomial f of degree t over $Z_q$ such that $P_i$ holds a share $x_i = f(i)$. The public key $y = g^y$ is global and known to all parties (and clients), and encryption is as in ElGamal above. For decryption, a client sends a decryption request containing $c_1, c_2$ to all servers. Upon receiving a decryption request, server $P_i$ computes a decryption share $d_i = c_1^{-x_i}$ and sends it to the client. Upon receiving decryption shares from a set of t+1 servers with indices $S$, the client computes the message as

$$m = H(\Pi_{i \in S} d_i \Theta \lambda^{S}) \Theta c_2 \quad \cdots \cdots \cdots (1)$$

This works because

$$\Pi_{i \in S} d_i \Theta \lambda^{S} = \Pi_{i \in S} c_i \Theta x_i \lambda^{S} = c_i \Theta \Pi_{j \in S} \lambda^{S} = C^x \quad \cdots \cdots \cdots (2)$$

Note that the decryption operation only requires the cooperation of n-t servers. This is an example of a non-interactive threshold cryptosystem, as no interaction among the parties is needed. It can also be made robust, i.e., secure against an active adversary. Such threshold cryptosystem can easily be integrated in asynchronous distributed systems; but many threshold cryptosystem are only known under the stronger assumption of synchronous networks with broadcast.

3. RESEARCH GAP

According to Rahman et al. [11], identity theft exploits a systemic weakness for identifying people, and as such a systemic analysis can be of value. In principle, there would seem to be two approaches possible for reducing identity theft: either making it more difficult, or making it less profitable. However, when the systemic response is taken into account, there may be conflicts between these two approaches: for example, actions which make identity theft more difficult may also have the effect of making it more profitable. For instance, a single barrier approach would involve developing a proof of identity which was extremely hard to forge. However, a single barrier is also a single point of vulnerability, and a very good proof of identity would induce so much confidence that if the rouge could forge it, he could get away with anything – thus making such a forgery, although difficult, very profitable.
Moreover, this paper proposes the development and widespread deployment of identity management system which employs two way (double) barrier for good proof of identity and reduced vulnerabilities.

4. PROPOSED SCHEME: BIO-THRESHOLD CRYPTOSYSTEM

The proposed scheme employs the use of biometrics and the threshold cryptography for prevention of online identity theft. The main focus of this model is to authenticate individuals before accessing service.

Merely username and passwords checking is not enough for preventing identity fraud.

Biometrics can be used by various organizations to increase security levels and protect their data and patents. The merit of biometrics is proven by endeavors of the G8 countries to apply it to prevent forgery of passports and other travel documents as part of their fight against terrorism.

Table 3: Illustration comparing Biometric types [9]

<table>
<thead>
<tr>
<th>BIOMETRIC TYPE</th>
<th>Fingerprint</th>
<th>Facial Recognition</th>
<th>Hand Geometry</th>
<th>Speaker Recognition</th>
<th>Iris Scan</th>
<th>Retinal Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Verification</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Identification</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Accuracy (4)</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Reliability (4)</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Security Level (4)</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Long term Stability (4)</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Acceptance (4)</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Ease of Use (4)</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Fingerprint Recognition involves taking an image of a person's fingertips and records its characteristics like whorls, arches, and loops along with the patterns of ridges, furrows, and minutiae. Fingerprint matching can be achieved in three ways (Maltoni et al., 2002):

- **Minutiae based** matching stores minutiae as a set of points in a plane and the points are matched in the template and the input minutiae.
- **Correlation based** matching superimposes two fingerprint images and correlation between corresponding pixels is computed.
- **Ridge feature based** matching is an advanced method that captures ridges, as minutiae capturing are difficult in low quality fingerprint images.

Rahman et al. (2010) opines that threshold decryption/signing is very useful in practice is because not only does it provide secrecy and reliability but also flexibility. Hence, sharing the secret key by multiple parties, each holds a share of the secret, can guarantee that decryption is done if and only if all parties agree to do it and therefore the scheme can give us a much higher level of security.

4.1 Implementation

Whenever a client wants to access a service online, authentication is done before client’s request will be honoured. Only on the basis of this will access be granted to all the subscribed service to client. This proves client’s authentication to server. Client first request authentication from the Authentication Server (AS) and/or database. The AS creates a “session key” (which is also an encryption key) basing on client’s password and a random value that represents the demanded service. Thus, the session key will then be used by the client to get master ticket to access services from the client server. An algorithm and a corresponding flowchart are designed to help in the implementation of the proposed system (as shown in figure1).

**ALGORITHM**

**STEP 1:** Start
**STEP 2:** Extract feature and authentication using the authentication server
**STEP 3:** Is fingerprint valid?
**STEP 4:** If YES, authentication server sends permission encrypted with client’s password and GO TO STEP 6
**STEP 5:** If NO, client is invalid and discard
**STEP 6:** Clients access services
**STEP 7:** Waiting time for reply
**STEP 8:** Number of reply = k. If YES, key can be regenerated and client send request to server
**STEP 9:** If NO, GO TO STEP 7
**STEP 10:** Stop
Identity thieves tend to steal twelve types of private personal information such as: credit card numbers, CW2 numbers (the back of credit cards), credit reports, social Security (SIN) numbers, driver’s license numbers, ATM numbers, telephone calling cards, mortgage details, date of birth, passwords and PINs, home addresses and phone numbers. This misuse of person’s data for impersonation and abuse of banking/financial services facilities is a growing concern in developed as well as developing societies. This paper therefore describes a proposed scheme that employs both the biometrics as an automated way of authenticating an individual and threshold cryptography for prevention of identity theft. Furthermore, this paper tends to be a basis for further research and designing of the using any suitable program for web-based applications.

**REFERENCE**


[5] Graeme R. Newman and Megan M. McNally (2005). Identity Theft Literature Review. Prepared for presentation and discussion at the National Institute of Justice Focus Group Meeting to develop a research agenda to identify the most effective avenues of research that will impact on prevention, harm reduction and enforcement


[10] Susan K. Langford (1996), Weaknesses in Some Threshold Cryptosystems. Atalla Corporation, 2304 Zanker Road, San Jose, CA 95131 E-mail: langfordsusan@tandem.com
