Abstract— Social Engineering is a way of targeting and exploiting human weakness to elicit and gain access to needed sensitive data. SE attacks are very common now a days. Sensitive and private information are taken away from the users even without their knowledge which even includes biometric information. Organizations tries to make their employees aware of possible SE attacks as well as they take preventive mechanisms against it. It is found that biometric data are more difficult to steal than passwords. Hence, biometric technologies are used over passwords in most of the areas where information requires high security. This paper is an eye opener to the fact that biometric information are also prone to SE attacks. The major biometric technologies such as fingerprint identification, iris scan, hand geometry, face recognition, keystroke dynamics, signature recognition and voice recognition are susceptible to prime SE attacks like phishing, watering hole, baiting, persuasion, pretexting, quid pro quo, tailgating, vishing and even physical attacks. This paper seeks to locate prevalent SE attacks which divulges into and steals the irrevocable biometric data. Updated technologies, giving proper awareness, education and training to employees, implementing multifactor authentication technologies, liveness detection mechanisms, challenge-response etc. may help to reduce SE menace and damages.

Keywords— Information Security, Social Engineering, Cyber Attack, Biometric Technologies, SE attacks, Cyber Security, Defense Mechanism, Hacking Techniques

I. INTRODUCTION

People use social media for different purposes and are prone to different types of cyber-attack. The privileged information can be secured using different techniques. To gain access to it, users are provided with credentials. As it is easy to hack login and passwords, biometric authentication found its way ahead. There are different cyber-attacks or traps that exist to steal these biometric data. Instead of going for traditional methods, some hackers make a trap for human beings based on their weakness [3]. The hackers gain sensitive and privileged information such as passwords, bank account details etc. by manipulating human beings.

Social Engineering is one of the ways used widely by perpetrators to exploit the human weakness or errors in order to elicit the needed biometric data or any confidential information to hackers or intruders [1]. As Kevin Mitnick said, “People are the weakest link in the security chain”. SE attack mainly occurs due to human errors rather than security vulnerabilities and hence it is highly dangerous. The whole idea of social engineering attack is to target the users associated within an organization, deceive the victim and then hack the targeted victim [11] through SE techniques for gaining biometric data.

We have done a research on how biometric information can be stolen using SE attack techniques. The objective of this paper is to give an idea that biometric information are also under the threat of SE attacks. This paper is organized as follows: Initially we provide the mainly used biometric techniques; then an overview of major SE attacks; followed by the analysis of possible SE attacks on biometric technologies along with scenarios; then some SE defense measures; and a conclusion.
II. STANDARD BIOMETRIC TECHNOLOGIES

2.1 Physiological Biometrics

2.1.1 Fingerprint Identification: Fingerprint identification is a non-invasive biometric technology in which it identifies, measures and analyse a person’s fingerprint[2][17].

2.1.2 Iris Scan: Iris scanning technology can capture the iris pattern quickly and it remains unchanged during an individual’s lifetime.

2.1.3 Hand based Verification/ Hand Geometry: In this method, the physical dimensions of the hand is captured and is used to verify the identity and authenticate an individual uniquely [6].

2.1.4 Face Recognition: Face authentication technology analyses, monitors, measures and captures the distinct characteristics of human face which can distinguish a person’s identity from one another [2].

2.2 Behavioral Biometrics

Behavioral biometric systems focus on the pattern of the behavior, movements and gestures of the person [2].

2.2.1 Keystroke Dynamics: Keystroke recognition is a behavioural biometric technology which can confirm a human identity by monitoring the uniqueness in the typing pattern of an individual on the keyboard [7].

2.2.2 Signature Recognition: Signature is a widely adopted behavioural biometric authentication technology which can recognise and identify the hand written or digital signature of an individual so as to confirm the identity of an individual [1] [2][15].

2.2.3 Voice Recognition: Every individual has unique voice pattern. The voice commands or phrases that we use instead of passwords will be recorded and stored in the system initially to which the commands would be later compared using Voice recognition software [2] [15].

III. PREVALENT SOCIAL ENGINEERING ATTACKS

Social Engineering milks the psychology of human beings. Some of the prevalent SE attacks are

3.1 Physical Attack: If the adversary uses physical means to search for sensitive data or to gather security information, then it comes under physical attack.

3.2 Phishing: It is an attempt to make users to give their sensitive information such as username, passwords, credit card information, or any other credentials to the attacker in a virtuous manner. In phishing, the users are tricked and make them believe something untrue [1].

3.3 Watering Hole: Here, the predator’s eye is on a group, instead of an individual. The attacker targets website/s which is/are frequently visited by a particular group or an organization and infects them with malware [3].

3.4 Baiting: It is a kind of phishing, which tempts victim to surrender their login credentials or other sensitive information for some goods or gifts [1] [5].

3.5 Persuasion: Giving a lot of false information about an unfamiliar situation easily allows a target to be persuaded forcing them to take illicit actions [1].

3.6 Pretexting: Here, an attacker builds a fake scenario to obtain privileged information from the victims [1].

3.7 Quid Pro Quo: It is a barter system in social engineering attacks. Here, the attackers offer some kind of services or benefit and the victims exchange or trade something for value [1] [5].
3.8 Reverse SE: Reverse SE is also a type of SE in which the attacker puts on the mask of a problem solver [1].

3.9 Tailgating: In tailgating, the attacker gets physical access to the site [13]. Here, the attacker may simply walks behind a legitimate person who has access permissions.

3.10 Vishing: Vishing, a combination of the words ‘Voice’ and ‘Phishing’, aims on gaining financial or personal information. The call may take the form of urgency which makes the victim to act without thinking.

IV. APPROACHES TO BREAK-IN BIOMETRIC DATA USING SE TECHNIQUES

Here we locate the possible SE attacks along with a scenario on significantly used biometric technologies.

4.1 Fingerprint

There are various possible ways to beat the fingerprint biometrics such as photocopying the image of a finger, making the clone of a fingerprint by taking close-up photo of the finger, fetch the fingerprint using tape, executing software attacks, organizing SE attacks and so forth. With a high quality photograph of a finger, the print of finger can be designed and created. This designed fingerprint can be transferred into a material, which can later be used to access or log into his/her account as a fake fingerprint biometric.

Scenario: An attacker may invite the user by offering a cup of tea and the fingerprint can be easily collected by the adversary even from the cup used by the victim. Then, this fingerprint can be used to make replicated copies of fake fingers which is then exploited to gain access to unauthorized data.

4.2 Iris Scan

In iris scanning systems, an encoded pattern would be derived from the iris and this encoded pattern is stored for future authentication purposes. To compromise iris scanning security, a high resolution photograph of the victim’s eyes is all they need. Keep a contact lens upon the iris in the printed image of the owner and show it in front of the iris scanner to bypass the security. A person’s dead eyeballs can also be used for bypassing the authentication. Physical attacks can be done to procure eyeballs for gaining access. As an improvement to the older systems the new systems detect eye movements along with the pattern. It is clear that a perfect high quality picture is good enough to pass around iris biometrics. A well woven pretext or reverse SE techniques can trap a person to allow an attacker to take his/her photograph.

Scenario: An attacker fools a person or a group of people by saying that he is a researcher and he needs to study about the size and types of human eye. He builds trust in them and invoke their helping nature. After befriending with them, he starts taking pictures of the eyes of the people with their consent. These high quality eye images can then be falsely used to bypass their iris biometrics.

4.3 Hand Geometry

A fake hand can be made by capturing the features of hand in a non-intrusive way. These artefacts can be extracted through SE attacks by tricking the user from an arbitrarily posed hand image, or from a video. Through SE, attacker will possess deep knowledge about the user internal characteristics and hence they will adopt any of the SE methods to collect the needed artefacts from the user. Once they obtain the needed artefacts, a fake biometric hand is contrived which is identical to the real shape of hand.

Scenario: An attacker impersonating as a bank employee may request a user to open a new bank account. As part of initial procedures to open an account, the adversary pretends to collect some data from the victim which may include the hand geometry of the victim. The employee who blindly trusts the attacker will allow the attacker to capture the hand geometry of the victim. The attacker will then save this data as a very high resolution image and later these artefacts would be used to effectually forge the identity of the victim.
4.4 Face Recognition

Here, the facial geometric features are used to uniquely identify and confirm the identity of an individual. It is not burdensome for the fraudster to obtain the photograph of a user from social media or a selfie picture or playing a looped video. An attacker tries to use a non-live image to capture the facial features in a non-invasive way to impersonate a targeted victim.

Scenario: An attacker or a group may come up with an offer of free medical camp to the employees in an organization. Then the attacker would be able to collect the required biometric data from the targeted victim who avails the free medical check-up facility.

4.5 Keystroke Dynamics and Signature Recognition

Both the keystroke and signature verification technology is based on typing pattern and rhythm of an individual on digital devices such as keyboard, mobile phones and other touch screen devices. So to forge keystroke or digital signature pattern, one has to imitate the same pattern and rhythm of a victim. It is very hard to learn the same pattern as it takes much time and patience. Even though imitating keystroke and signature pattern is beyond the limits of possibility, we cannot consider it as an impossible task.

Scenario: If an attacker invents background stories and impersonate as a trainee and asks the victim to teach the typing techniques, the adversary can closely watch the typing style of the victim. All the typing styles can be closely observed or he may even capture a video for further detailed study. If the attacker undergoes constant training of the victim’s typing pattern, gradually he can imitate the same.

4.6 Voice Recognition

People use voice recognition to access their gadgets or to gain entry privilege to one’s office cabin or use some commands for gaining access to something which requires security. The attacker initially tries to know the particular keyword or command used by the user for access privileges. Then they makes the victim speak out that particular word or phrase through any of the SE techniques and record their voice. The recorded voice can be used in future for fraudulent purpose. The attacker could even record the voice command which is overheard.

Scenario: The attacker masquerades as a tech support staff member and approaches the employees telling that he came to install an updated version of anti-malware in all the systems of that organization. And hence the employees are asked to utter the voice command to unlock the device. The adversary records the voice commands and later he exploits it for security breach.

<table>
<thead>
<tr>
<th>Physical Biometrics</th>
<th>Behavioral Biometrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerpint Identification</td>
<td>Keystroke Dynamics</td>
</tr>
<tr>
<td>Iris Scan</td>
<td>Signature Recognition</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>Voice Recognition</td>
</tr>
<tr>
<td>Face Recognition</td>
<td></td>
</tr>
<tr>
<td>Physical Attack</td>
<td>✓</td>
</tr>
<tr>
<td>Phishing</td>
<td>✓</td>
</tr>
<tr>
<td>Watering hole</td>
<td>✓</td>
</tr>
<tr>
<td>Baiting</td>
<td>✓</td>
</tr>
<tr>
<td>Persuasion</td>
<td>✓</td>
</tr>
<tr>
<td>Pretexting</td>
<td>✓</td>
</tr>
<tr>
<td>Quid pro quo</td>
<td>✓</td>
</tr>
<tr>
<td>Reverse SE</td>
<td>✓</td>
</tr>
<tr>
<td>Tailgating</td>
<td>✓</td>
</tr>
<tr>
<td>Vishing</td>
<td>✓</td>
</tr>
</tbody>
</table>

TABLE 1. VULNERABILITY OF BIOMETRIC TECHNOLOGIES TO SE TECHNIQUES
Table 1 shows the possible vulnerabilities in biometric technologies due to SE attacks.

V. DEFENSE MECHANISMS

5.1 Defense mechanisms against SE attack in general

5.1.1 Train and educate employees: Employees must be trained [1] [8] enough to know the value of passwords and other information they are dealing with. They should be made aware of the standard policies and procedures [9] of the company. Provide resistance training [8] to the employees who connect directly with the clients and the outsiders such as customer service executives, receptionists, front office personnel, secretaries etc. to harden them against SE attempts. Develop an intranet site and keep posting the new types of attack approaches, its countermeasures, incident happened outside and inside the organization, steps taken by the organization to prevent it, etc.

5.1.2 Motivatie and Provide Persistent reminders: Make the training a compulsory one and a matter for promotion. Reward the employees whoever withstand the attacks. The impact of training seems to decrease as days goes by because it is human tendency to forget things. Provide the employees regular reminders about hacking attempts taking place inside and outside the organization and keep it updated with new preventive techniques which would make them alert and conscious.

5.1.3 Use software protection and Detect malicious data: Install some software which could recognize if any manipulation is going on or if any attack attempt is taking place in the network, or email or website or any other digital media. Monitoring tools [8] also warns the organization about the malicious activities and possible threats.

5.1.4 Mock Excercises and Documentation: Include the questionnaires, scenarios and arguments a social engineer might use. Documentation helps to share experience with the employees [4].

5.1.5 Understand your Emotion: Employees must be instructed to contact back the suspicious person. Instead of answering a call or replying a mail soon, the employee can verify if the number of the caller or website address is genuine or not [4].

5.2 Defense mechanisms to mitigate the risk in biometric data

5.2.1 Updated Technologies and Facilities: Keeping a centralized entry of all the attack attempts will definitely help the employees to refer it if they come across any suspicious activities [8]. By implementing intrusion detection system or anti-malwares, the vulnerability caused by a software can be prevented to a certain extent [10].

5.2.2 Liveness Detection Mechanism: Liveness detection system distinguishes between a live human sample and a copy of a feature provided by artefact [12] [14] [16]. An effective defense mechanism against face, fingerprint and iris forgery is liveness detection/testing. We can even use hardware [12] to sense life.

5.2.3 Using Hardware: Detect temperature, pulse and blood pressure for finger print liveness detection [12]. Analyse the movement of the face for face recognition. Measure involuntary constrictions and dilations of the pupil for liveness detection in iris scanning. Synchronize lip movement with voice [14] in voice recognition systems. Since it is difficult to duplicate the exact size and shape of sweat pores in a mould, implementing a sensor which can detect sweat pores is a good practise to ensure more security.

5.2.4 Randomizing biometric measurements: Instead of reading the same biometric data every time for granting access, ask the user to provide a random subset of biometric measurements [12] such as right middle finger followed by left little finger.

5.2.5 Challenge-response: Try to capture the response of fingers by passing a small impulse current to the finger [12]. This test will outwit the use of artefacts. Users can also be asked to repeat a particular phrase, blink their eyes, nod heads or present specific fingers to the sensor in order to confirm the authenticity of the user [16].
5.2.6 **Multiple Biometrics**: Even though multiple biometrics adds complexity to the system, adding one more biometrics would definitely make it harder for the hacker to spoof [14]. Keep multiple as well as different biometrics for authentication purposes such as voice and iris.

5.2.7 **Multifactor Authentication**: One of the most effective SE attack defense mechanism is to build different layers of protection. Incorporating two or three biometric authentication techniques [14] such as voice, iris and fingerprint for privileged access would be a successful security measure. Secure each biometric information by encrypting it.

VI. **CONCLUSION**

We have systematically presented here the currently used biometric technologies for authentication purposes and revealed the major SE attacks. Security means knowing about what and whom to trust. In order to avoid and prevent the SE attacks, an individual should know about the significant trending SE traps. We explained how these attacks are viable in stealing the biometric information without human knowledge. We cannot fully overcome such attacks and hence more ideas are to be identified to resist and prevent SE attacks. It is always better to take some preventive measures against SE attacks which we have discussed in detail. Thus, it is imperative to build an awareness among the people to know about the growing leaps and bounds of SE attacks. We need to develop more software to detect and prevent SE attacks as humans are prone to emotions. Multi layered defense mechanisms is a one word solution. Make hacking a burdensome task for the hacker. On the whole, this work provides a new perspective to understand, perceive and assess the SE attacks and its ramifications in entire spectrum of biometrics as well as the risk mitigation strategies in a multi-dimensional manner.

**REFERENCES**


