International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.02, February 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

SURVEY ON COMMON ATTACK VECTORS AND COUNTERMEASURES OF FINGERPRINT SYSTEMS

ALI FATHI ALI SAWEHLI[1], NEIL ANDREW RUSSELL VIDOT[2]

[1,2]BSc (Hons) Cyber Security, Asia Pacific University, Kuala Lumpur, Malaysia

ABSTRACT

Fingerprint system has several vulnerabilities that lead to the security issues. These vulnerabilities can be categorized into two parts which are direct attacks and indirect attacks. The direct attacks mean that the attack will be performed into the sensor of the fingerprint directly which can be such as spoofing attack. Indirect attack means the attacker is targeting either the channel that establishes the connection between the sensor and the system or by attacking the database storage or the algorithm that do the extraction and the matching processes of verification and identification. The indirect attacks that have been discussed in this article are denial of service "DoS", reuse of residual, replay attack / false data injection, unauthorized template modification and interconnect threats. Then how to mitigate these risks by implementing a series of procedure such as liveness detection, multi biometric feature, multi factor authentication, physical security and making good policies. Finally, this article explains all the mentioned above.

Keywords:Algorithm, Common attacks, Counter measures, Fingerprint systems, Identification, Verification.

I.INTRODUCTION

Nowadays, biometric technology becomes more popular day after day because of the new and convenient method that they provide to get access to the secure environment. This technology has brought a significant improvement to the information system security field. The main aim is to provide an alternative way of authentication method instead of using the old way of authentication such as using username and password which that may lead to the user forget the password or the account is being hacked. There are many types of biometric technologies methods such as fingerprint, iris, face, retina, hand, palm and signature, Moreover, these technologies can be used by embedding them with the electronic devices which can be found such as smart phones. In addition, biometric systems are used in many places nowadays such as at the airport that help to take the passenger's identity such as fingerprint and iris.

In a school, hand, palm system has been used to take the attendance of the students instead of wasting time to take it in the traditional way.

Furthermore, each type of biometric systems has own way of authentication process and each one has own strength and weakness. In this research, the fingerprint system technology is chosen as the main focus and discussing the threat vectors and how to mitigate from them. The main purpose of choosing fingerprint is considered to be as the highest one that heavily used in among of biometric technologies. The acceptance rate among the people is very high. So, this article highlights the threats that may lead to exploit the system and common issues [1].

II. HOW FINGERPRINT SYSTEM WORKS

The authentication process of the fingerprint can be divided into four stages which the verification decision is made after passing these stages. The diagram below is illustrating the process.

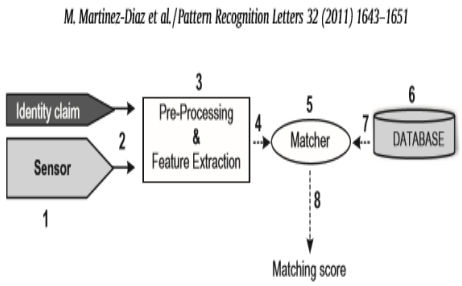

Figure 1: Biometric Verification System

a) First, the sensor will capture the live-scan image of the person that is trying to authenticate.
b) Second, the image will be processed into extrication method to create a template of the fingerprint or model.
c) Third, the template will be compared with the client's identity by using the template database.
d) Fourth, the fingerprint system will accept the user or not based on the matcher [1]

III. COMMON ATTACKS IN FINGERPRINT

Nowadays, most researchers are doing researches about the biometric technologies, especially in fingerprint part. One of these researches, they discovered that there are many types of vulnerabilities and attacks have been found on the fingerprint systems in the last years. These attacks can be categorized into parts which are direct attacks and indirect attacks. Each category has own way to attack the finger printer systems [2]. These attacks are being discussed below.

1) DIRECT ATTACK

Direct Attack means that the attacker attacks the finger printer system by providing some counterfeited biometrics to the sensor. Furthermore, this attack can be also known as "Spoofing Attack". However, the main thing that gets this kind of attack to be successfully done is when the sensor of the fingerprint cannot detect whatever the live template is a fake or the original of the client. Before diving into how the spoofing attack works, we need to know how the fingerprint systems by introducing some terms [3].

a) First, the user needs to provide his identity of his finger to the fingerprint system which is called as "identification process".
b) Second, the system will claim the identity from the user and store it into the database on the system.
c) The claimed identity of the user is called as "stored template" which will be compered on every time when the user try to authenticate.
d) If the result of the comparison is true "accepted" as genuine and if it is false "rejected" as an imposter.
e) Furthermore, there is a thing called as False acceptance rate "FAR" which helps to avoid as much as the system can of the imposter acceptance [3].

1.1)SPOOFING ATTACK

The spoofing attack can be defined as the way of gaining unauthorized access of the fingerprint system by coping, stealing or replicating the biometric trait. In addition, this attack can be considered as the high-risk attack to the fingerprint system that does not require a massive knowledge about the system which also can any person implement this attack. Because there is no need to know how the system works such as the extraction and matching algorithms that are used and the ways of encryptions that the system uses [3]

Figure 2: Fake made of Latex Direct Method

Spoofing attack is an old discovered attack that the first time had been implemented in the 1920s by Alert Wehde. When he was an inmate at Kansas penitentiary, he used his experience in the photography and engraving to produce a gummy of finger print from the latent fingerprint. The latent fingerprint was highlighted using forensic methods and the photograph was taken. The photograph was used to etch the print onto a copper plate that was used to produce the fake fingerprint on the surfaces. In the last years, there were many investigative researches had been conducted to study how the fingerprint system is dealing with the spoofed finger print. One of the research was by synthesizing finger print using a silicon and the plastics. Furthermore, the devices that had tested were six optical and the solid-stat commercial sensors. The result of the research was 5 sensors permitted to gain unauthorized access into the system from the first trying, but the sixth sensor was from the second time. In addition, there were another research that had been conducted by Matsumoto et al. The experiment was similar to the research above, but it's produced by fabricating gelatine. In this research, eleven commercial sensors were used with a success rate more than 60 % [3].

Furthermore, the finger print spoofing ways can be categorized into kinds which are “cooperative/direct” casts and “non-cooperative/indirect casts”. In the first type which is direct casts, the fake finger print can be created by a cooperative with the owner of the fingerprint. On the other hand, the second category which is indirect casts and the fingerprint is made without the direct cooperative of the owner such as latent finger marks on the surface without notice which helps to fabricate the fake finger print to get access to the systemThe soft materials that help to take a copy of the finger to produce the fake finger print from the user which are as wax, play doh, plaster or dental impression material. All these materials can be used to produce a mould [3].

2) INDIRECT ATTACK

Indirect attack is the way of attacking a system by knowing the applications and features that the system is running them. In the biometric technology field, the attacking method is not restricted to spoofing attack only "direct attack", but it can be such as attacking the stored template database, storage channel intercept and data inject, denial of service "Do's attack", replay attack / false data inject, reconstruct template data, unauthorized system access, modify access rights, override feature of the extraction and matching attack. This type of attack cannot be implemented by zero knowledge about the finger print system and its different from the direct attack type. So, the attacker should have a good knowledge about the system [4].In this section, common indirect attacks of the fingerprint system will be highlighted to get know what threats that affect the systems.

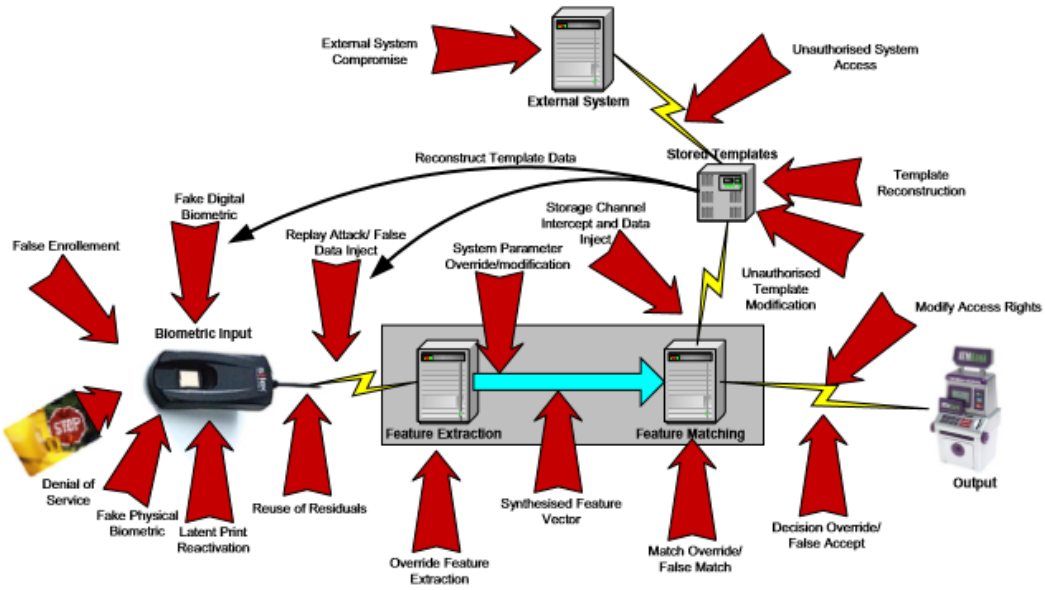

Figure 2: Common Indirect Attacks

2.1 System Vulnerabilities

System Vulnerability is one of the most recently attack that effect the systems which leads the attacker to get into the system. There are many areas that the vulnerability can be found in it which are: -

a. The operating system "OS" of the fingerprint system.

b. Storage management system.

c. The applications that finger printer system use.

d. Hardware and sensor software

To mitigate the risk of the system vulnerability is by keeping installing the patches of the operating system and the applications that the fingerprint system use [4]

2.2 DOS ATTACK

Denial of service "DOS" is a type of attack that affects the biometric systems. Furthermore, it considered as most of one dangerous attack. Physical damage or power loss can be caused to the biometric systems. As a result, the system data may be corrupted by the adverse environments such as light, heat and dust, which can decrease the performance of the fingerprint sensors. In addition, there are different ways to perform this type of attack which by generating signals such as electrical signals or radio frequency. So, by generating these signals, the data quality will be decreased immediately. For optical sensors can be attacked by using the portable strobe light or by splitting a liquid on sensors. In general denial of service attack can be discovered quickly. Finally, to mitigate this type of attack, is by providing a feature in the fingerprint system that notify the administrator that there is something suspicious, such as alarm and using alternative handling procedure and taking backup regularly [4].

2.3 REUSE OF RESIDUALS

Reuse of residuals attack which means that the attacker can attack the local memory of the fingerprint system. In general, in every system, the memory retains some of the last processes for a period time. When comparing this with fingerprint system, the system also saves some extraction processes or the templates. As a result, the attacker can reuse this template and modify to be as valid fingerprint template. To mitigate against this attack can be clearing the memory consecutively to provide better defence [4].

2.4 REPLAY ATTACK/ FALST DATA INJECT

Reply attack / False data inject can be considered as a way of the man in the middle attacks. This type of attack is happening when the connection is established between the sensors and the fingerprint system. So, the attacker can intercept the traffic and inject the false data. Furthermore, there are many finger print systems that do not provide an encryption, which means the data will be in clear text and the attackers can get to the traffic easily. In addition, this attack can be summarized into three stages which the first stage is to intercept and copythe sensor transmission, and the second stage is to modify the data and the third step is to replay the signal. These are considered as the main three stages, and it depends on the fingerprint system which may use an encryption technique. So, the attacker needs

to decrypt and re-encrypt to perform this attack. To avoid this risk, there are some finger print systems that are using some encrypted protocols which provide more security value into the system.

2.5 SYSTEM INTERCONNECTION THREAT

System interconnection means that the system has some established connections to another server system to provide a service or services such as providing a cloud service. This connection is called as an external system interconnect. There is a possibility that the external system got compromised. So, the attacker can target the connected systems which can be the fingerprint system one of them. The connection channel will be attacked in the first step in order to gain access and compromise the fingerprint system. When the external system interconnection is required, it would be better to choose the external system with high security feature to mitigate these types of attacks and make the fingerprint system is safe [4].

2.6 UNAUTHORIZED TEMPLATE MODIFICATION

There are many ways to store the template in the fingerprint system which can be on the fingerprint reader, a sensor or inside the fingerprint system. So, the attacker can modify or add or delete the template if the fingerprint system is vulnerable to this attack. In addition, to implement this attack can be by performing a denial of service attack "DOS" which helps to make a damage on the date or assigning modified template to existing users. To mitigate this type of attack, it is better to store templates and the date in encryption way such as a hash format. So, the authentication process in the matching, the hash values of the sample and the template will be compared in order to gain an access to the system. Finally, there is no safe way that grantees that the date cannot be modified at all.

2.7 MODIFY ACCESS RIGHTS

This attack is very common which is called as modify an access right or user privilege escalation. This attacker has gained an administrator privilege and his target is to upgrade the privilege to some users. Furthermore, upgrading the finger print system parameter such as the false rate can be possible to perform by the attacker. This attack can be found in different systems such as biometric systems, windows system, Linux system and web server.

III REDUCING THE RISKS

There are many ways that help to mitigate the attacks that the finger print system can be exposed to them. In this section, the defence vectors will be highlighted [5].

3.1 LIVENESS DETECTION

Liveness detection is very useful to mitigate a direct attack such as spoofing attack. This is the type is to make sure that the fingerprint sample is presented with the live and real people when providing it to the reader and approve that is not an artificial or from a cadaver. (Martinez-Diaz,2011). This can be by providing this feature in the fingerprint system which are: -

1- Finger print perspiration patterns measurement.

2- Three-dimensional feature which helps to be against pose.

3- Eye detection.

4- Thermal measurement.

3.2 MULTI-BIOMETRIC FEATURES

Providing multi biometric features that make the authentication process more complex and it is difficult to crack and break down. To add another complicity layer to finger print system isby requiring also the iris scan. The concept of multi biometric system can be applied for the sensitive systems and places that require more security. (Martinez-Diaz,2011)

3.3 MULTI FACTOR AUTHENTICATION

Multi factor authentication is a way of using password, PIN, token and smart card. This technique can be used with fingerprint technology, which if the user is injured in his/her fingerprint, he/she can recover the access by entering the second multi factor. Furthermore, this technology can be used with a multi biometric feature which by combing both techniques together to gain access to the system. This argument on how to use these authentication methods depends on the sensitivity of the system that the user trying to get authenticated on it. (Martinez-Diaz,2011)

3.4 PHYSICAL SECURITY

The internal attack can be considered as more effective and dangerous way to compromise any system in comparison with an external attack. So, if the attacker has a physical access to the fingerprint system or any type of biometric systems, can attack the system easily by performing the above-mentioned attacks. So, to defeat these attacks, can be providing a limited access to the fingerprint reader, supervised operation or presence security guards. In addition, providing regular check on the sensors to check that there is no latent material of the sensor. Monitoring finger print system or server room can be also by using CCTV that cover all the areas. Furthermore, there are many ways that prevent and limit the physical attacks [1].

3.5 POLICY

Policy is standard of rules that manages the process on the company. Furthermore, these polices can be a security policy. A security police is that illustrates the welcomed and unwelcomed activities that can be implemented in the company's systems which enhance the security. Thereare many frameworks that are available for information system security, such as ISO and NIST. These organizations have done an incredible job on how to manage the security values of the company. Furthermore, it enhances also in how to protect the biometric system and especially

the finger print system by how to protect the equipment such as the sensors and the database storage from being attacked. So, the policy is a very important aspect that should be taken in the consideration [1].

IV CONCLUSION

The biometric systems are growing and more features and new methods have been discovered. As a result, the attacking methods also are growing with the same line of biometric system growth. Fingerprint system is one of biometric technologies that came out. It provides a good authentication method which is by using the authenticator's finger. This technology is the same as the other technology, which means it has advantages and disadvantages. The main advantages of fingerprint system are provided to dispense the old authentication methods such as the username & password. Every person has own minutiae points of his/her finger, which makes the attacker's job a little bit harder. In other hand, if the template of the fingerprint is stolen, the hacker can spoof it and try to gain access to the system by using the spoofed fingerprint of the victim. Second disadvantage is that if the hacker gained it, the victim cannot change his/her fingerprint. To sum up, when designing any biometric system or fingerprint system, especially, the security risks and threats must be taken into consideration such as mitigating from denial of service attack, replay attack/ false data injection attack and more. Furthermore, training the administrators that monitor and control, biometric systems against these attacks. Finally, this article has highlighted these major attacks and how to mitigate from them.

V ACKNOWLEDGMENT

The authorswould like to share gratitude to Mr Umapathy Eaganathan, Lecturer in Computing, Asia Pacific University, Malaysia for the constant support and motivation which helped us to participate in this International Conference and also for journal publication.

REFERENCES

[1] Martinez-Diaz, M., Fierrez, J., Galbally, J. and Ortega-Garcia, J. (2011). An evaluation of indirect attacks and countermeasures in fingerprint verification systems. *Pattern Recognition Letters*, 32(12).

[2] Espinoza, M., Champod, C. and Margot, P. (2011). Vulnerabilities of fingerprint reader to fake fingerprints attacks. *Forensic Science International*, 204(1-3).

[3] Biggio, B., Akhtar, Z., Fumera, G., Marcialis, G. and Roli, F. (2012). Security evaluation of biometric authentication systems under real spoofing attacks. *IET Biometrics*, 1(1).

[4] Roberts, C. (2007). Biometric attack vectors and defences. *Computers & Security*, 26(1), pp.14-25.

[5]Edward Guillen, Lina Alfonso, Karina Martinez and Marcela Mejia. (2012). Vulnerabilities and Performance Analysis over Fingerprint Biometric Authentication Network. Proceedings of the World Congress on Engineering and Computer Science 2012 Vol II WCECS.