Vulnerability Analysis Of Fingerprint Biometric Authentication Systems & A Proposed Secure Architecture.

Divyajyoti Das (Author)
Bachelor of Technology, School of Computer Science & Engineering
Kalinga Institute of Industrial Technology, Bhubaneswar

Abstract

Fingerprint Biometrics based authentication systems are becoming increasingly popular, compared to traditional systems that are based on tokens or knowledge (e.g., password). The primary reason being they offer greater security and convenience than traditional methods of personal recognition. These secure authentication systems are vulnerable to attacks, which can decrease their security. In this paper we uncover the vulnerabilities associated with Fingerprint Biometrics authentication systems and propose a secure architecture to ensure the security of the systems. The key focus being Side Channel attacks which includes threats associated with the feature extraction, Signal Processing, Storage and Comparison unit inside the Finger Print Biometrics device. The secure architecture to fight against the above mentioned vulnerabilities in the systems consists of an algorithm implemented at processor level to secure the system against Side Channel Attacks and an algorithm that shall be a part of the Signal processing unit to ensure secure matching of fingerprints thus ensuring the internal security of the system.

1. Introduction

Fingerprint Biometric recognition systems offer greater security and convenience than traditional methods of personal recognition that are based on token or knowledge (e.g., password). Biometric systems not only offer greater security but also provide speed and accuracy in the authentication process. These features are making them the most trusted and reliable authentication systems across the globe. With the growing invention of more and more powerful embedded processors, Biometrics recognition systems are certainly the future of personal recognition and authentication. But are these systems secure themselves? Fingerprint Biometric recognition systems are vulnerable to attacks which can decrease their security. The widespread use of these systems is making their security more and more important.

2. Vulnerability Analysis of Fingerprint Biometric Recognition System

One of the most significant disadvantages of the biometric recognition system is that they cannot be easily recollected. For example if one of the fingers is used as a password, once it is compromised, it can never be used again since it is almost impossible that a fingerprint can be changed, which means it is compromised forever. Moreover, since one person only has a limited number of fingers, different applications might use the same fingerprint. A person’s biometric stolen from one application could be used in some other applications. Thus the secure storage of the biometric template is great importance. Earlier the biometric template such as fingerprint was usually stored on central server during enrolment. The biometric signal captured by the sensor was sent to the server and the matching steps were performed by an application running on the server. The security of the template couldn’t be guaranteed as attacks could occur during transmission or on the server. These flaws led gave birth to embedded biometric recognition systems. Embedded biometric recognition systems provide a solution to the problem by moving the signal processing and matching engines from the server to the embedded device. The embedded system process and match the signals and only the result is transmitted to the server. This approach can be very effective in avoiding the attacks on communication and server. Now the big question is, how secure are embedded biometric systems?

To ensure the secure storage of biometric template it is encrypted using a secure key before being stored. As soon as the input signal is received from the sensor, the matcher decrypts the template and comparison is done. However, there are attacks which can still extract the secret key and thus unveil the template. The key reason being physical implementation of an algorithm provides an attacker with some valuable information. Variations in timing, power consumption and electromagnetic radiation can be used to link to the internal state of the processor, and hence the secret data. These attacks are called as Side Channel attacks and can be a huge threat to the security of the entire Biometric authentication system. Among the many Side Channel Attack techniques, Differential Power Analysis (DPA) is the most power one. Differential Power analysis uses statistical analysis and error correction to extract information from the power consumption which is correlated to the secret data.

3. Fingerprint Matching

Fingerprint matching is an important component of the authentication process. The two types of fingerprint matching techniques include graph based and minutiae based. In embedded fingerprint biometric devices minutiae based approach is commonly used. The main reason being minutiae of the fingerprint are believed to be the most reliable and discriminating features. Moreover, the template size of the biometric information based on minutiae is quiet smaller than graph based fingerprint matching. This approach is very important for saving memory and energy on embedded devices. The above mentioned procedure can be extended with one important time saving step, namely classification. It is used in cases where the database containing fingerprints is so large that a fingerprint with all the images is too time consuming. Fingerprints can be classified based on the following patterns: loops, whorls and arches. Using this approach the fingerprint need not be matched with all the fingerprints in the database. The first stage is the fingerprint enrolment phase. Next pre- processing is done so as to improve the quality of the image taken by the fingerprint sensor. The minutiae are extracted from the processed image and stored in the database.. This process repeats itself resulting in the generation of a 'live template' Lots of work has been done in the area of minutiae based fingerprint matching. Some use the local structure of the minutiae to describe these characteristics. This approach offers high processing speed and robustness to rotation and partial prints. The local structure has less distinct features as it represents only some parts of the whole minutiae set. In Alignment based matching algorithms take use of the shape of the ridge connected to the minutiae. This is likely to improve system accuracy. This approach results in larger template size because the associated ridges for each minutia must be saved. Some other researches combine both the local and global structures.

4. Side Channel Attacks

Transistors are voltage control gates. When voltage is applied to the gates, current flows across the substrate and charge is delivered to the additional circuitry. Integrated circuits are constructed from a collection of individual transistors, each with their own voltage control gate. A microchip is an integrated circuit consists of millions of transistors. A chip's overall electrical activity represents the electrical activity of the individual transistors. The power consumed by a chip correlates to the computation being performed. These measurements are the basis of SPA (Simple power analysis) and DPA (Differential power
analysis) attacks. ARF(Argon Fluoride) emissions by a chip can also yield similar results.

5. Simple Power Analysis

Simple Power Analysis begins with simple observation of device's direct power consumption. These measurements can be taken by a standard digital oscilloscope. . The security of a chip relies on keeping the keys secret. If attackers can find the keys they can perform unauthorized activities such as forging smart cards, committing piracy and making fraudulent payments. Automated SPA attacks can be completed against the vulnerable device in a few seconds with less than 1000 dollars of equipment.

6. Differential Power Analysis

DPA is a statistical method to correlate information collected across multiple power consumption measurements. DPA is a more sophisticated attack than SPA and is used when individual bits cannot be seen because of noise, measurement errors and countermeasures. These measurements are statistically analysed to determine the key. The statistics used in DPA are extremely powerful and can extract keys even if individual traces contain large amount of noise that would make direct SPA type analysis impossible. The information from these combined observation reveal several bits of the key and can reveal the entire key thus compromising the vulnerable device.

In a typical DPA attack, the objective is to extract the secret key used in a device. The process begins with reference average trace of the device's power consumption waveform. DPA enables an attacker to guess the key by solving for a few bits of the key at a time. The attacker first guesses the value for some key bits. The guessed keys are used to predict computation intermediates. If the key bits are guessed correctly, the resulting differential trace will show spikes in the locations correlated to the predicted intermediate. If the key portion is guessed incorrectly the resulting trace will be flat except for some random noise. By repeatedly applying this process the attacker can use differential traces to solve for key fragments which can then be assembled to revel the entire secret key.

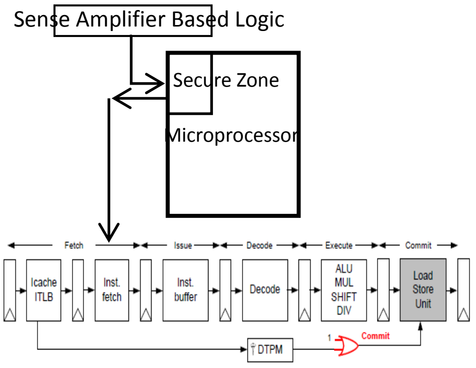
7. Existing Countermeasures

With the growth of Side Channel Attack techniques, a number of countermeasures against Differential Power Analysis have been proposed. Still these countermeasures act ineffective against the advanced versions of Differential Power Analysis. For Instance, Random Process Interrupts can be synchronized by integration techniques and advanced Differential Power Analysis can handle masking techniques. Another technique usually used to avoid DPA attacks is Random Power consuming operations. However, these operations merely lower the side channel information and could be disabled through tampering.

The above mentioned countermeasures attempt to conceal the power variations at architectural or algorithmic level whereas they themselves originate at logic level. Thus implementing the sensitive parts of a crypto processor at logic level, whose power consumption independent of the signal transitions, removes the foundation of Differential Power Analysis. Sense Amplifier Based Logic (SABL) is one such logic style. However, this method though effective in avoiding DPA attacks to some extent is not cost effective to implement.

8. Proposed Secure Architecture

The secure architecture that we have designed to ensure the security of fingerprint biometric devices starts from the processor level itself. In the processor level a secure part is designed and the rest part is encrypted. The keys used to encrypt are stored in the secure part of the processor. The secure part is designed in Sense Amplifier Based Logic style. The logic is encrypted by inserting some additional gates into the design such that only on applying some specific input to the gates, the design produces correct output. During working the secure part verifies the instructions. It decrypts the encrypted units if instructions are correct. The instructions are then executed by the processor. If they are incorrect processor does not execute them. The figures below depict the encrypted processor pipeline which forms the base of the secure zone inside the microprocessor. Inside the secure zone runs an encrypted processor pipeline with Dynamic Trusted Platform Module as a secure part Load Store Unit (LSU) is encrypted. This part is made functional only when the instructions are correct. It remains non-functional if incorrect instructions are received.



It is this secure part that shall deal with all operations relating to the sensitive biometric template. This includes accessing of the template data as well as computation related to those values. The secure fingerprint matching algorithm is discussed below which shall run in the secure part. Algorithm Given a minutiae M, the local structure of it is described as a feature vector.

L={d1,d2,……,dN,a1,a2,….aN,v1,v2,….,vN,H}-------------- ---------------(1)

Where, n= Number of neighbours taken into consideration during matching.

H=Local ridge direction of minutia M.

D (n=1,2…N) describes the distance between the selected minutia and its nth nearest neighbour.

A(n=1,2…N) is related to the radial distance between M and its nth nearest neighbour

V(n=1,2….N) represents the related position angle of the nth nearest neighbour. The proposed matching algorithm calculates how similar neighbourhood of one minutia in the input fingerprint is to that of one in the stored template.

If they are found similar, then they are taken as matched minutiae pair and they are used to calculate the final matching score. In this case selection of neighbourhood is highly essential for each minutia. When two minutiae are compared, the relative position and angles of its 6 nearest neighbour minutiae are investigated. We can now re write equation 1 as-

L={{d1,a1,v1},{d2,a2,v2},………..{dn,an,vn},H}----------- -------------------------(2)

L'={{d1',a1',v1'},{d2',a2',v2'},…….{dn',an',vn'},H'}---- --------------------------(3)

To decide whether or not M and M' are a matching pair, a 4dimension range box is set for {d,a,v,H}.In the first step local ridge directions of the two minutiae are checked. If {H-H'} > del.H (del.H represents delta H) M and M' are not matched. Hence, the matcher looks for another pair.

If |di-dj|<=del.d , |ai-aj|<=del.a , |vi-vj|<=del.v ---------------- -------------------(4)

In case the conditions in step 4 are satisfied, the 'i' th neighbour of input minutiae M and 'j' th neighbour of template minutiae M' are considered marked. After a thorough scan of the total number of marked neighbours,it is accumulated as A. Following this procedure let us assume we have total number of matched minutiae pairs as B. If this number is above a set threshold TH, then it is considered as a matched pair. Considering the number of input and template as INP and TEM respectively, the final matching score is calculated as:

Score= B/ Max (INP,TEM)

The algorithm described above is a secure fingerprint matching algorithm which shall run in the secure part of the microprocessor ensuring security of the signal processing and comparison sections. In order to provide added security to the system against we propose another algorithm that shall protect the processor against Side Channel Attacks.

Algorithm To keep track of the switching activity, an adder-subtractor arrangement is used which keeps track of the series of 1,0 or 0,1 in the FSRs (Feedback Shift Registers). Instead of calculating the switching activity of the FSR in each cycle, the counter tracks it by considering only the bit that exits the used cipher and the bit that enters it. If a series of 1,0 or 0,1 is inserted and a series of 1,1 or 0,0 is removed the switching activity of the counter increases by one. If a series of 1,0 or 0,1 is inserted and a series of 1,1 or 0,0 is removed, the counter value increases by one. Finally if 1,1 or 0,0 is inserted and a series of 1,0 or 0,1 is removed, the switching activity decreases by one.

```
If phase=initialization
 then
CPlevel=level //CPlevel is the current power level.
PPlevel=initialState //PPlevel is the previous power level. Else
If CPlevel==PPlevel + 1 OR PPlevel=initialState then
Wait for K clock cycles in CP level
 Else
  If SA<SAlevel1
 then       //SA is Switching Activity
  CPLevel=level1
End if
  If SAlevel2<=SA<SAlevel3
then
   CPLevel=level2
    End if
    If SAlevel3<SA
   then
    CPlevel=level3
End if
 End if
```

9. Experimental Results

A AF-2 CMOS imaging sensor was used for capturing the biometric fingerprints. The processor used in the core was a Cortex M4 processor. The two algorithms, the Sense Amplifier based logic and the secure core architecture was implemented. The Secure fingerprint matching algorithm yielded very less false acceptance rate, approximately 0.1%. The Sense Amplifier based logic used with the Power Masking Algorithm also masked the power consumption activity of the system to a great extent.

10. Conclusion

The secure architecture provides security at the processor level as well as logic implementation level, thus enhancing the security of the whole system. With the growing use of fingerprint biometric systems for personal identification and authentication, our secure architecture is certain to make biometric devices more trustworthy of use. The unique thing about this approach is that the system is protected at the processor level itself. It is where the core security lies which in turn creates a secure platform for implementation of algorithms.

11. References

[1] Developing Advanced Signal Processing Software on Cortex-M4 Processor by Shyam Sadashivam .

[2] Cryptography and Network Security by Forouzan.

[3] A Document on Biometrics by Prof. A. Chidanand, IIT Kanpur.

[4] Data Communications and Networking by Fourouzan

[5] Unvelling Biometrics by S.K Rath, IIT Bombay.

[6] Fingerprint Matching – An Experimental Approach by Prof. Ryan Williams, Columbia University.

[7] P. Tuyls, B. Škorić, and T. Kevenaar, eds. Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting. Springer-Verlag, London, 2007.

[8] A. Cavoukian and A. Stoianov, Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy, March 2006. http://www.ipc.on.ca/index.asp?navid=46&fid1=608

[9] National Science and Technology Council Subcommit- tee on Biometrics and Identity Management, Biometrics in Government Post-9/11: Advancing Science, Enhancing Operations, Aug. 2008; www.ostp.gov/galleries/NSTC%20 Reports/Biometrics%20in%20Government%20Post %20 9-11.pdf.

[10] A.K. Jain, P. Flynn, and A.A. Ross, eds., Handbook of Bio- metrics, Springer, 2007.

[11] H.C. Lee and R.E. Gaensslen, eds., Advances in Fingerprint Technology, 2nd ed., CRC Press, 2001.

[12] J. Feng, “Combining Minutiae Descriptors for Fingerprint Matching,” Pattern Recognition, Jan. 2008, pp. 342-352.

[13] A.A. Ross, K. Nandakumar, and A.K. Jain, Handbook of Multibiometrics, Springer, 2006.

[14] S. Pankanti, S. Prabhakar, and A.K. Jain, “On the Indi- viduality of Fingerprints,” IEEE Trans. Pattern Analysis and Machine Intelligence, Aug. 2002, pp. 1010-1025.

[15]D.R. Ashbaugh, Quantitative-Qualitative Friction Ridge Analysis: An Introduction to Basic and Advanced Ridgeology, CRC Press, 1999.

[16] D. Maltoni et al., Handbook of Fingerprint Recognition, 2nd ed., Springer, 2009.

[17]R. Cappelli et al., “Fingerprint Image Reconstruction from Standard Templates,” IEEE Trans. Pattern Analysis and Machine Intelligence, Sept. 2007, pp. 1489-1503.

[18] National Research Council of the National Academies, Strengthening Forensic Science in the United States: A Path Forward, National Academies Press, 2009.

[19] Thalheim, L., Krissler, J., Ziegler, P. (2002) Body Check. c’t heise online. 11/2002, page 114 .

[20] Anderson, R. (2001) Security Engineering. 1. p. Ch 3. Wiley. Canada. 612 pages. ISBN 0-471-38922- 6.

[21] Precise (2003) Precise Biometrics 100 SC scanner data sheet.

[22] Leyden, J. (2003) Biometric sensors beaten senseless in tests. The Register. 1/2003.

[23] Schneier, B. (1999) Counterpane Labs. Biometrics: Uses and Abuses. 8/1999.

[24] R. Bolle, J. Connell, S. Pankanti, N. Ratha, and A.W. Senior. Guide to Biometrics. Springer, 2003.

[25] Nifty gadget or something more sinister? The Guardian, January 11, 2005