HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Nguyen Huu PHUOC DAI
phuoc.daitt@bgk.uni-obuda.hu

FINGERPRINT DEVICE (SUPREMA) IS SAFE OR NOT?

Abstract

Fingerprint is one of the most important biometric techniques to identify personal information of an individual. For example: log in computers, network, a car and so on. This technique is primarily because people can operate and install this system easily. Finger authentication system is divided into four steps such as: using sensor, feature extraction, template matching and decision about authentication. In this article, the author used some measures in order to evaluate the safety of biometrics device, especially in Suprema device.

Az ujjnyomat alapú az egyik legfontosabb biometrikus azonosítási technika az egyén beazonosítására. Alkalmazható például: számítógépekbe történő bejelentkezéshez, hálózatokhoz, autókhoz, és így tovább. Ez a technika több szempontból is előnyös, az emberek könnyen tudják nem csak telepíteni de működtetni is a rendszert. Az ujjnyomat hitelesítési rendszer négy lépésből áll: szenzor alkalmazása, tulajdonság-kinyerés, sablon azonosítás és végül döntés az azonosságról. Ebben a cikkben a szerző bemutatja a biometrikus technológiákat, majd egzakt méréseket alkalmaz annak érdekében, hogy értékelje biometrikus eszközök a biztonságát. A méréseket Suprema eszközzel végzi.

Keywords: *biometrics, biometric device, fingerprint ~ biometria, biometrikus eszköz, ujjnyomat*

INTRODUCTION

In the past few years, biometrics used to identify people by using some figures from human being‘s physiology as fingerprint, hand geometry, iris, face recognition, voice and so on. Moreover, a biometric system is vitally a pattern recognition system that acquires biometric data from an individual, extracts features set from the acquired data and compares them with the template set in the database [1]. It is also used to verify individuals in groups that are under suspect. The biometric system based on the information extracted from the differences of people ‘s trait. Furthermore, biometric recognition is used for enrollment, verification and authentication of biometric template in biometric system [2]. In the enrollment process, the individual's fingerprint are enrolled into the system by Suprema device. In verification process, the system is verified query human's trait with enrolled human's own biometric charecteristics. In authentication process, the system validates individual by comparing the entire enrolled fingerprints with the templates stored in the database. Fingerprint method is considered as the most reliable method because of some reasons such as: low cost of equipment, low time of procedure. In fact, in United states has Integrated Automated Fingerprint Identification system where above 51 million of criminal's fingerprints are stored and about 1,5 million of civil fingerprints. Regarding that system database, it makes the crime investigation easier and minimizes the time a lot [3]. In short, while fingerprint technology offers a lot of benefits for the users, there are also many problems that should be aware of.

LITERATURE REVIEW

Definition

According to [4], biometrics technology is a term which came from Greek and this word can divide into two roots: "bio" – means life and "metrics" – to measure. It is a new authentication method to identify the user in three ways: something that person knows (password), something the person has (key, special card) and something the person is (fingerprints, footprint).

Moreover, biometrics technology is a method to verify or recognize the identity of an individual based on physiological or behavioral characteristic [5]. Based on the context, biometric has 2 modes: verification mode and identification mode.

Verification mode: the biometric system authenticates a person's identity by taking his/her own biometric template stored in the database and comparing with the captured biometric data. In this system, an individual is required to use a PIN- personal identification number as username, a smart card, etc. and it manages one-to-one comparison to identify whether the captured user's template is true or not. This mode is mostly used for positive recognition and it prevents multi-users using the same identity [6].

Identification mode: in contrast to verification mode, this mode indicates the individual by searching all templates of the users in the system database for a match. In another way, this system conducts one-to-many comparison to identify user's identity and rejects someone if he/she is not enrolled in the database. Especially, this mode doesn't require the users have a PIN as verification mode and its purpose to prevent a single person from using multiple identities [7].

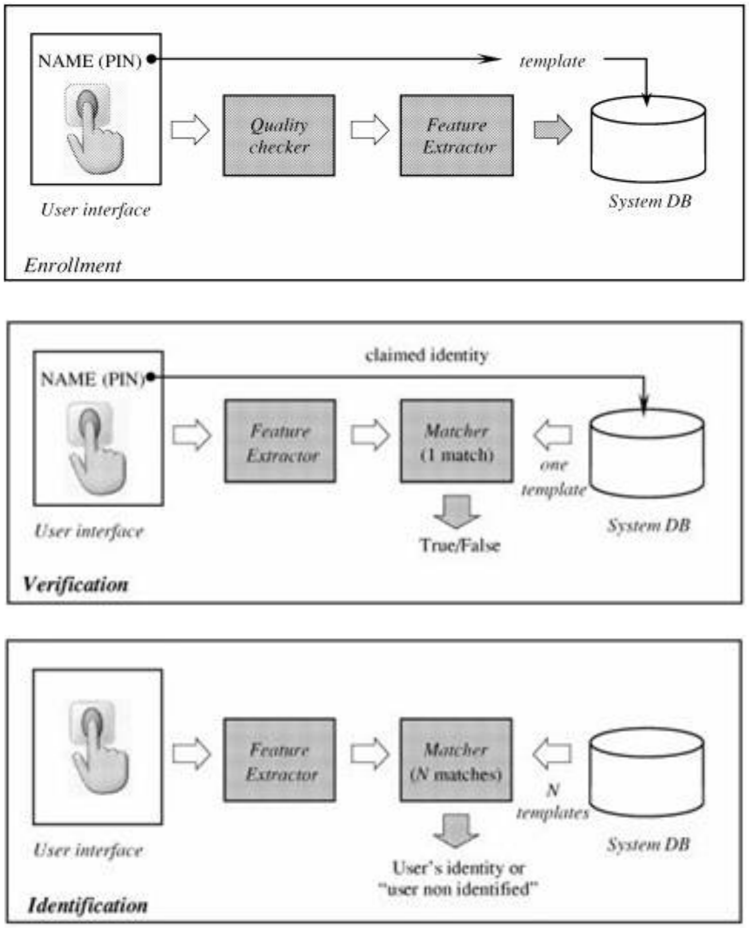


Figure 1: Block diagram of enrollment, verification and identification (source: Anil K. Jain et al.) [8]

Classification

There are two main categories of biometrics authentication system: physiological type and behavior type [3].

Physiological type

Fingerprint: is one of the oldest and popular method in biometrics authentication system. It used the picture of user's finger pattern from any surface that person touches. It can be said that fingerprints are strong evidences in investigating the crimes.

Face recognition: the system uses the 2D or 3D digital image of an individual. This method based on some factors of human being's face such as: distance between eyes, width of the nose, depth of the eye sockets, the shape of the cheekbones and the length of the jaw line.

DNA: similar to biometric based fingerprints, this method widely used in identify the criminals. It consists of four bases: Adenine (A), Guanine (G), Cytosine (C) and Thymine (T) which make DNA code of an individual. However, it only has one exception with the twins because of the same DNA structure.

Palm print: it refers to the palm region image of user's hand. It is similar to fingerprints and iris recognition method but their size is bigger and it has a limitation of using mobile devices. This method has three main factors as wrinkles secondary lines, ridges and especial in principle lines of user’s palm. Each different user’s palm contains texture, indents and marks which are used to authenticate one with another.

Hand Geometry: the difference between one person and the other is the geometric shape of their hands, for example: height, length of the fingers, distance between joints, shape of the knuckles and surface area of the hand [9]. This method based on these factors in order to recognize the users but it is seldom used today because with young children, their geometric shape of the hands can change through time.

Iris recognition: the aim of this method is to analyze the iris’s outer boundary where it meets white sclera of the eye, pupillary boundary and the center of pupil. This system makes the process fast and secure, but it also has some drawbacks for instance, it is impossible to recognize individual when scanning user’s eyes from a distance or user’s eye problems (blindness and cataracts).

Behavior type

Typing Rhythm: a technology to recognize the way of individual’s typing on a keyboard. The main features of this technology such as latencies between successive keystrokes, duration of each keystroke, finger placement, pressure applied on keys and overall typing speed. When user access to the system, he/she types (login name, password…), and keystroke will capture data and compare with captured template in database.

Gait: this technology depends on the way of people walk, style of walk, pathology, etc. In another way, gait recognition analyze the movement parameters as knee, ankle movements, angles and spatial-temporal elements as the length or width of steps, the speed. Then, this technology figures out the difference in correlation between those parameters from one person to another person.[10]

Voice: Voice recognition is one of the fastest methods to authenticate individual. The voice is gained from different person because the wave of sound which comes from different human throat and mouth. The tone of the sound is established by tongue, gums, teeth, lips, the size of stream and so on. This method takes user’s speech and stores them in database. Then in identification process, the captured sample is compared to the template in database, if the result matches, that person can be verified [11],[12].

Benefits

According to [4], biometric system offers some advantages in order to authenticate the users in the system. Firstly, the users can’t pass their biometric characteristic to the other easily as they do with their passwords or smartcards. Moreover, it is more convenient than passwords/cards because the users don’t need to remember the hard-to-memorize passwords or keep them. Secondly, with the boosting of biometric technology, it creates a new and secure method to make highly accurate verifications of individuals and it cannot be stolen as traditional authentication (password, card, token, and the like). In fact, the attackers may not break the user’s fingerprint/iris pattern even using the fake or artificial biometric characteristics because most biometric techniques based on the thing that cannot be stolen or forgotten. Thirdly, this method can reduce management costs. For instance, with the new authentication method, the administrators don’t need to reissue or issue password/card/token when the users have problems or losing them. Therefore, it can reduce a lot of time and cost for management. Finally, biometric authentication system may be faster than traditional method, for example: using iris-based recognition may take 2 or 3 seconds while find the smart card or typing the right password, it may take 4 or 6 seconds.

Drawbacks

Like all technology, biometrics comes with a lot of advantages; however, it also has some drawbacks as the cost, time-consuming, unsuitable with someone. Firstly, different biometric technology needs to have a range of cost to deploy in workplace. Moreover, individuals sometimes concern waiting in a long line in order to get inside the building, school or company. Secondly, some biometric method can't apply with someone [13], for example: fingerprint is impossible to authenticate someone with no hands, face recognition fails to identify individual for whole life because their face will change through time and age. Furthermore, when biometrics are common in everywhere in our life, all information are stored in database; therefore, there is no more privacy.

RESEARCH CONTENT

Methodology

This research mainly focuses on the way of biometrics device protecting user's database. Based on the purpose research, hypotheses are formulated at the beginning of the research and tested in this study.

Hypothesis

- H0: Biometrics device is not safe and it can be exploited from the hackers via sniffing attack.
- HA: Biometrics device is safe and it cannot be exploited from the hackers via sniffing attack.

The author used the fingerprint device – *Suprema* to do some experiments (figure 2).

Figure 2: Suprema - fingerprint device [14]

Regarding to this device, it can handle maximum 10000 templates and 5000 users. Firstly, the author registered the some test fingerprints templates into this device by using Biostar v.162 and Biostar server config software to connect between the device and computer via TCP/IP protocol (figure 3), (figure 4).

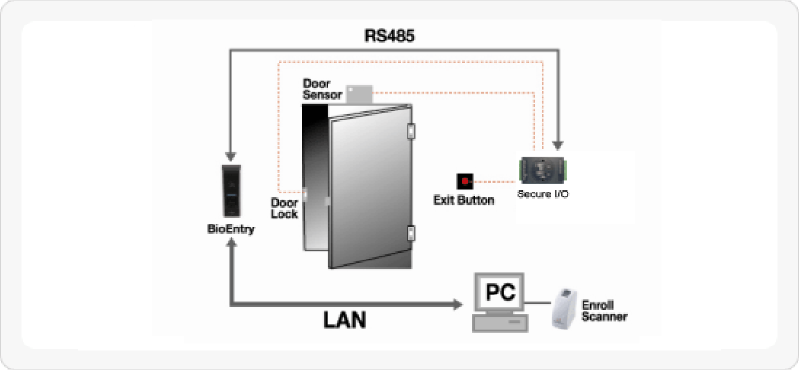
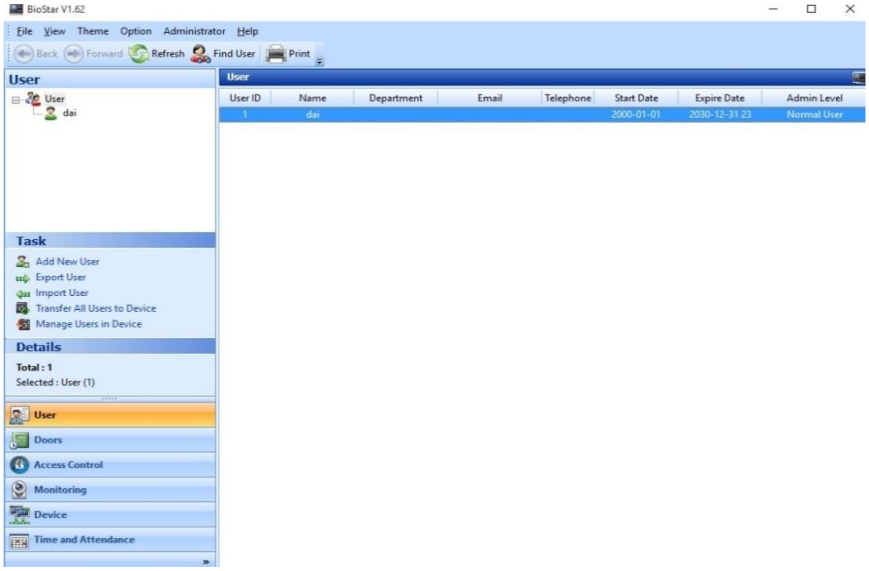


Figure 3: Standalone-secure configuration [14]



User

User ID	Name	Department	Email	Telephone	Start Date	Expire Date	Admin Level
1	dai				2000-01-01	2030-12-31 23	Normal User

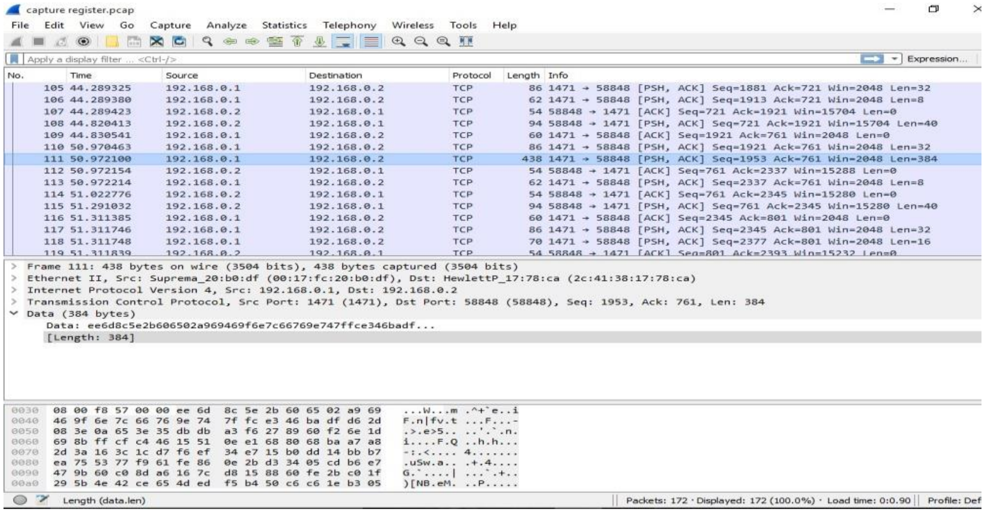
Total : 1
Selected : User (1)

Figure 4.Biostar’s interface. (source: own data)

Secondly, the author used Wireshark to capture the data between biometrics device and computer when they transmit the packets during register’s session. The packets are the binary signals. Moreover, the captured data are analyzed to find the biggest length of packets (the encrypted information of the user’s registration) between biometric device‘s transaction and laptop (figure 5). The registered templates are saved into *Suprema* memory through *Biostar v1.62*. Then, the next step is that deleting registered templates on the device’s memory. Finally, the author tried to play back the captured signal via the biometrics device in order to evaluate the security of the device.

Research result

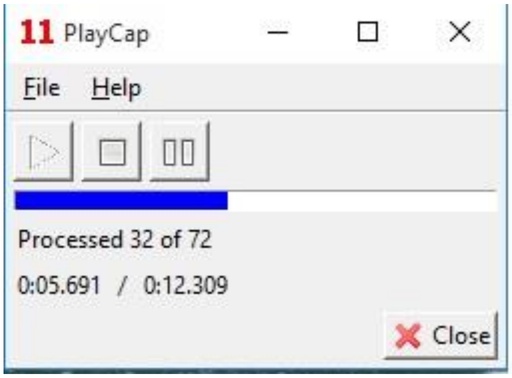
The author used *Wireshark* tool to capture the signal when the client register from the machine to computer (figure 5).


capture register.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…

```
No.     Time         Source         Destination    Protocol  Length Info
    105 44.289325    192.168.0.1    192.168.0.2    TCP         86 1471 → 58848 [PSH, ACK] Seq=1881 Ack=721 Win=2048 Len=32
    106 44.289380    192.168.0.1    192.168.0.2    TCP         62 1471 → 58848 [PSH, ACK] Seq=1913 Ack=721 Win=2048 Len=8
    107 44.289423    192.168.0.2    192.168.0.1    TCP         54 58848 → 1471 [ACK] Seq=721 Ack=1921 Win=15704 Len=0
    108 44.820413    192.168.0.2    192.168.0.1    TCP         94 58848 → 1471 [PSH, ACK] Seq=721 Ack=1921 Win=15704 Len=40
    109 44.830541    192.168.0.1    192.168.0.2    TCP         60 1471 → 58848 [ACK] Seq=1921 Ack=761 Win=2048 Len=0
    110 50.970463    192.168.0.1    192.168.0.2    TCP         86 1471 → 58848 [PSH, ACK] Seq=1921 Ack=761 Win=2048 Len=32
    111 50.972100    192.168.0.1    192.168.0.2    TCP        438 1471 → 58848 [PSH, ACK] Seq=1953 Ack=761 Win=2048 Len=384
    112 50.972154    192.168.0.2    192.168.0.1    TCP         54 58848 → 1471 [ACK] Seq=761 Ack=2337 Win=15288 Len=0
    113 50.972214    192.168.0.1    192.168.0.2    TCP         62 1471 → 58848 [PSH, ACK] Seq=2337 Ack=761 Win=2048 Len=8
    114 51.022776    192.168.0.2    192.168.0.1    TCP         54 58848 → 1471 [ACK] Seq=761 Ack=2345 Win=15280 Len=0
    115 51.291032    192.168.0.2    192.168.0.1    TCP         94 58848 → 1471 [PSH, ACK] Seq=761 Ack=2345 Win=15280 Len=40
    116 51.311385    192.168.0.1    192.168.0.2    TCP         60 1471 → 58848 [ACK] Seq=2345 Ack=801 Win=2048 Len=0
    117 51.311746    192.168.0.1    192.168.0.2    TCP         86 1471 → 58848 [PSH, ACK] Seq=2345 Ack=801 Win=2048 Len=32
    118 51.311748    192.168.0.1    192.168.0.2    TCP         70 1471 → 58848 [PSH, ACK] Seq=2377 Ack=801 Win=2048 Len=16
    119 51.311839    192.168.0.2    192.168.0.1    TCP         54 58848 → 1471 [ACK] Seq=801 Ack=2393 Win=15232 Len=0

> Frame 111: 438 bytes on wire (3504 bits), 438 bytes captured (3504 bits)
> Ethernet II, Src: Suprema_20:b0:df (00:17:fc:20:b0:df), Dst: HewlettP_17:78:ca (2c:41:38:17:78:ca)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
> Transmission Control Protocol, Src Port: 1471 (1471), Dst Port: 58848 (58848), Seq: 1953, Ack: 761, Len: 384
v Data (384 bytes)
    Data: ee6d8c5e2b606502a969469f6e7c66769e747ffce346badf...
    [Length: 384]

0030  08 00 f8 57 00 00 ee 6d  8c 5e 2b 60 65 02 a9 69   ...W...m .^+`e..i
0040  46 9f 6e 7c 66 76 9e 74  7f fc e3 46 ba df d6 2d   F.n|fv.t ...F...-
0050  08 3e 0a 65 3e 35 db db  a3 f6 27 89 60 f2 6e 1d   .>.e>5.. ..'.`.n.
0060  69 8b ff cf c4 46 15 51  0e e1 68 80 68 ba a7 a8   i....F.Q ..h.h...
0070  2d 3a 16 3c 1c d7 f6 ef  34 e7 15 b0 dd 14 bb b7   -:.<.... 4.......
0080  ea 75 53 77 f9 61 fe 86  0e 2b d3 34 05 cd b6 e7   .uSw.a.. .+.4....
0090  47 9b 60 c0 8d a6 16 7c  d8 15 88 60 fe 2b c0 1f   G.`....| ...`.+..
00a0  29 5b 4e 42 ce 65 4d ed  f5 b4 50 c6 c6 1e b3 05   )[NB.eM. ..P.....

Length (data.len)          Packets: 172 · Displayed: 172 (100.0%) · Load time: 0:0.90    Profile: Def
```

Figure 5. Signal in registration session. (source: own data)

After using *Playcap* tool to play back the signal from the captured data to computer many times, the biometric device couldn't recognize the user's authentication which is registered it before on the device. Therefore, the biometric device rejects the user's fingerprint.



```
Processed 32 of 72
0:05.691  /  0:12.309
```

Figure 6. Play back signal to biometric device (source: own data)

In summary, regardings to the results of the attacks to the fingerprint device (figure 2), we accept *HA:* the biometric device is safe and it cannot exploit from hackers via sniffing attack.

CONCLUSION

Fingerprint plays an important role in authentication user's identification. With the benefits of this technology, it makes easier for the users and the implementers to deploy this technology in many aspects. The main contribution of this research is to evaluate the safety of biometrics device. Through the above analysis, this paper showed that biometrics device brings many benefits for the users. Furthermore, the fingerprint is quite safe and security. In the future work, the author uses some other measures to evaluate some different biometric device in order to ensure the safety and security of biometric devices.

References

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, 2004.

[2] E. Mordini and D. Tzovaras, *Second Generation Biometrics: The Ethical, Legal and Social Context: The Ethical, Legal and Social Context (Google eBook)*. 2012.

[3] A. Babich, "Biometric Authentication . Types of biometric identifiers," pp. 1–56, 2012.

[4] C. Republic, "Biometric Authentication — Security and Usability," *Adv. Commun. Multimed. Secur. IFIP TC6TC11 Sixth Jt. Work. Conf. Commun. Multimed. Secur. Sept. 2627 2002 Portorož Slov.*, vol. 100, pp. 1–13, 2002.

[5] B. Miller, "Everything you need to know about biometric identification," *Pers. Identif. News 1988 Biometric Ind. Dir. Inc., Washingt. DC*, 1988.

[6] L.O'Gorman, "Seven issues with human authentication technologies," *Proc. Work. Autom. Identif. Adv. Technol.*, no. New York, pp. 185–186, 2002.

[7] D. Kumar and Y. Ryu, "A brief introduction of biometrics and fingerprint payment technology," *Proc. 2008 2nd Int. Conf. Futur. Gener. Commun. Networking, FGCN 2008*, vol. 3, pp. 185–192, 2008.

[8] J. Wayman, J. Wayman, A. Jain, A. Jain, D. Maltoni, D. Maltoni, D. Maio, and D. Maio, "An Introduction to Biometric Authentication Systems," *Biometric Syst.*, pp. 1 – 20, 2005.

[9] "Global Security org, Hand geometry and Handwriting. Available: http://www.globalsecurity.org/security/systems/biometrics-hand.htm"

[10] J. Boyd and J. Little, "Biometric gait recognition," *Adv. Stud. Biometrics*, no. July, pp. 19–42, 2005.

[11] "Authentify voice biometric authentication. Available: http://authentify.com/solutions/authentication-concepts/voice-biometric-authentication/"

[12] M. Khitrov, "Talking passwords: Voice biometrics for data access and security,"

Biometric Technol. Today, vol. 2013, no. 2, pp. 9–11, 2013.

[13] V. Burger, “Assignment 1 Biometric authentication”, thesis, 2005.

[14] https://www.supremainc.com/en/AccessControl-TimeandAttendance/Biometric-Devices/BioEntry-Plus

[15] https://www.supremainc.com/en/AccessControl-TimeandAttendance/Biometric-Devices/BioEntry-Plus)