Two-Way Continual Authentication Model

Carlos Fabián Lugani

LIA - Laboratorio de Informática Aplicada – Sede Atlántica –
Universidad Nacional de Río Negro
clugani@unrn.edu.ar

Summary. Authentication is a process by which a person using a personal computer, information system or device, defines its identity, and therefore, such system grant access based on predefined permissions. The use of biometric devices, IoT devices, wearable technology and other similar devices, define present authentication methods as weak and requires a level of mutual authentication so that both actors trust each other granting who they claim or seem to be. This paper addresses that information systems and/or devices that should validate their identity in the same way users do. Additionally, due to the increasing information security incidents, there is a risk that one of the actors, during the connection process, might be an impostor instead of a truly actor. For this reason, the authentication method should be a continuous and ongoing process in order to counteract with the security risks mentioned above.

Key words: authentication, identity management, security, IoT

1 Introduction

Need-to-Use is the primary baseline that defines who can and who cannot access and use a specific resource. At first, there is a person with a genuine interest who is allowed to use a system or a personal computer. Normally, it is well understood that the person knows where such system is, because the system is always located in the same place or can be unambiguously identified. There are systems that are not located at a defined site, but they normally provide a service for multiple devices and they are constantly changing. This is why the difficulty in the identification of systems will increase due to the different scenarios and the technological progress.

Normally, authentication involves the action that a person executes on an information system so that such system gives access to a specific information or allows to execute several predefined actions. All the actions that a person can execute have been previously programmed or enabled and therefore, the scopes of those actions are already known.

The verification of the user's identity more frequently used implies a simple method based on a username and a password. However, this identity verification is a very basic method because there does not exist strong verifications to validate if the password used truly belongs to the person who claims to be. Even though there are several

biometric technologies in order to increase the level of trust to verify a person's identity, they have not been widely adopted due to different factors, such as:

- Limitations for achieving cost-benefit implemented solutions.
- Lack of knowledge from actors or lack of information assessment leading to a loss of confidentiality, integrity and availability.
- Overconfidence when no incidents related to information security are occurring (originated by intruders or intrusion actions), or lack of information related to previous registered incidents caused by intruders in the past.

Taking into account all the issues mentioned above, this paper focus on a new approach on the authentication concept, by considering it as a method where every actor has the responsibility to provide confidence over other actors about its authenticity.

This is the reason why present systems are becoming more complex and not only do they have data about people and companies, but also they can control key functions of a human being as its heart system [1] or when people's lives depend on such key systems as: airplane flight self-control, drones traffic, automated control of robots, street traffic and motorized self-driving vehicle [2].

2 Major Difficulties

The model proposed can be better understood with the following example where a variety of actors with different interests can be appreciated regarding the authentication process among stakeholders.

- In the first place there is a vehicle equipped with state-of-the-art technology such as: driver/owner identity recognition, self-driving technology, access to the Internet and the traffic control information system, medical and security emergencies. There would be, as well, associated systems providing data which would identify the car and its driver as part of the traffic control system network.
- The driver gets out of his car at a shopping centre, he gives his car specific instructions for self-parking. When the driver leaves the shopping centre, he indicates his car to wait for him at the front door by means of a device connected to the Internet (cell phone or a wearable device).
- This particular example presents several types of associated identity verifications:
  - The car system must verify that the real owner is sending the message.
  - The car system must verify that the real owner is approaching the car so that letting him open the car's door and,
  - The owner must verify that the car is his own and no other person's car. This is the reason why computer/system authentication is the primary baseline for the owner's physical and personal security.
- The examples mentioned above are part of the authentication method established between two actors, however there would exist some other systems such as those one person can interact with, as the following example:

- You are driving your car and the system gets a message that there is a traffic jam and the car system gives the driver another alternatives to make the better driving choice.
- In this case, it is important to take into account the authentication process from the car to the traffic control system and the authentication from the traffic control system to the car. Any kind of mistake in these authentication process would make the system unreliable putting the actors at risk.
- It is also possible that the driver has a car accident leaving him unconscious, and in this case, the car's system sends information about the driver's health condition to a medical emergency system. This is the reason why the verification of the information reliability and user's identity is a primarily baseline.

According to the items mentioned above, the authentication process not only should it be only in one-way, but also a two-way technique is required, because both actors should verify the other actor effectively and unmistakably. This example shows the first concept of this paper that deals with the authentication process on both directions or named as two-way authentication technique.

Continuing with the difficulties exposed above it should be taking into account an important issue related to the information security point of view. Regarding information security, it is possible that a device/system or part of them can be forged once the communication was established. This can happened due to two reasons, the presence of multiple devices interfering instructions or signal messages that are not for the proper recipient, or the presence of fake devices replacing the original ones by the use of fraud, scams or even more serious situations such as spying or terrorism activities.

2 People Identification

In order to identify people into personal computers and different devices, there are several methods of authentication. There are software-based and hardware-based identification systems. These identification systems are being used when a person need to access a personal computer, an ATM, some Internet of Things devices, when accessing a building or a country. For all these cases, the identity must by verified. The identity is assessed and verified according to the established security levels. Therefore, every authentication action must be previously analysed regarding its associated risks. It is important to analyse these concepts in order to continue with other advanced or strong authentication methods or considering a combination of different methods. Particularly, identity verification risks should be assessed over weak methods of verification leading to an information leakage and also unauthorized physical and/or logical access. In this case, there existed not only the error of granting an improper access, but the user confidence of having granted this access to the proper user. This example shows that this authentication control is deficient.

For example, when a person logs in a personal computer he/she uses a password that could be a word, passphrase or a pattern drawn on the cell phone display – also some devices have fingerprints readers. Therefore, we have two types of authentication methods.

At a primary level of authentication, a person can be identified by some information he knows, although someone else can obtain and/or guess this information by different tricky methods. Consequently, the identity of a person cannot be truly verified.

In stronger levels of authentication, where is possible to identify different parts of the body, the authentication is called biometric authentication. Although this method is safer regarding its verification phase, it shows some difficulties, for example some people's fingerprints impressions are difficult to be clearly identified, and in the case of facial recognition systems, such systems can be modified, or when regarding to voice recognition systems, the voice to identify can be recorded for future cybercrimes. We have to take into account that biometric readers are sensitive to external agents such as water or dirt, making them useless and, therefore, this type of authentication cannot be used in every situation.

The following items show the different techniques that can be used for the present example [3]:

Digital fingerprints: this is the oldest identification technique, fingerprints reading and error recognition rates have been improved, and however, this technique cannot be used in every case.

Iris recognition [4]: this is the most accurate method for recognition because the algorithms used lead to an efficient matching search. The iris does not change and it is protected from accidents or dirt compared to other parts of the body.

Face recognition: this system is not frequently used because it presents different kind of false positive authentications due to several factors as deficient amount of light, distance and age as well.

Hand geometry recognition: this system reads the whole hand including fingers length, wrinkles and, in recent investigations, the shape of veins. [5]. However, there exist some problems regarding people suffering from specific conditions where hands or fingers cannot be accurate recognised making it difficult an accurate reading of the hand, also hand readers are too big.

Voice recognition: there are multiple applications and researches where voice is recognised by the means of different patterns. A training process is required before starting with this authentication method but it presents a high accuracy rate of 100%. [6] [7] [8].

Smell recognition: this method does not need any kind of physical contact but the person should be at a short distance from the reader making this a secondary verification phase [9].

Some other verification methods can be wearable devices. Such devices are electronic devices attached to clothes or accessories and they interact with the person carrying them. These electronic devices can be connected to some other devices in order to carry out an action previously programmed. Some examples are smartwatches, sneakers with GPS system, bracelet controlling vital signs, or clothing.

Taking into account the examples mentioned above, it is necessary to carry out a detailed analysis on the use of these devices or biometric systems for personal recognition. Such analysis should bear in mind that some people are reluctant to these type of biometric recognition by considering them an intrusive method. In this case, the

best verification method could be the use of different verification methods, so that the error rate would not be significant.

3 Components verification

Normally, the systems do not identify themselves to the people. In fact, people consider that if the system is where is supposed to be, that is enough for verifying its identity. For example, when using an ATM located at a bank, the user considers it as a trusted ATM. However, sometimes there are occasions when people can be deceived by fake ATMs.

When we are dealing with mobile devices and the Internet of Things (IoT), we do not consider its physical location, since these devices are portable and can be found in different locations.

Additionally, The Internet of Things devices are supposed to interact with other similar devices or central systems. Therefore, it is of paramount importance the verification of these devices with the other ones in order to assure the proper operation of the entire system. As an example of a significant authentication method, we can mention the airplane identification system and its interaction with the air traffic control system at land, where security and verification of the different actors is of critical importance.

These systems should consider other systems authentication methods when connecting to such systems in order to provide or deliver information. These verifications should have, as in the case of people, multiple sources of verification. For example, although existing a software authentication, it is needed a physical component (i.e. a short range radio label on most devices). This label should send a verification by the use of radio frequency (RFID: Radio Frequency Identification, or NFC: Near Field Communication) so that the different systems would be verified and managed by other devices, as if they were managed by the actors located at a short range distance. According to the information mentioned above, authentication is the most appropriate verification method using, at the same time, a combination of devices from different origins.

4 Two-Way Identification Technique

So far, the authentication case of people interacting with other people or other devices has been presented. According to this information the topic of two-way authentication method is introduced.

¿Why is it important that people and systems need to identify themselves reciprocally?

We have an evident answer if we are taking into account the new technologies in mobile devices, IoT devices and, specially, those devices connected to the human body, helping and/or directly performing some vital functions. Nowadays, bioprosthesis are being designed by private companies and universities [10] to help the

handicapped perform different activities or to maximize such activities (exoskeleton). These devices would become parts of the human body and would have their independent mobility. At the same time, these bio-prosthesis would be communicating their activities to other systems, and receiving information from these activities with different degrees of priorities. These inter-connections, its authentication, action capability, security maintenance for exchanging information between the different actors and the ability of these actors, will be part of that security device. This aspect is very important regarding its use by the people.

Considering these difficulties, it is important to contemplate that the verification performed by a person needs to verify he/she is using the correct device. In this case, the person should verify and check identities in an easy but secure way. This previous situation can include third parties connected to the same device such as some kind of networks or the Internet. For this reason, it is of primary importance to consider security issues related to connectivity.

5 Connection Continuity (Availability)

The second important aspect presented in this paper is related to continual authentication. Normally, systems need a logging process or entering a password to have access to such system only one time at the beginning of a session or work day. After that, it is supposed that the person who has accessed the system is always the same user, but the session could expire due to a long period of inactivity. However, even though the control process of inactivity can take a short time, during this period, the user could have changed as well as the original system.

This is the reason why a continual authentication process is required, as we have not to be totally confidence that after having performed the first contact, it would be not necessary to do further authentications in order to effectively be sure that the original person and system remain connected and no identity theft has occurred.

It is also important the way the connection is established, and depending on the methods used it is necessary to implement different control levels. In the first place, the connection between two different actors is considered safe or unsafe.

In the first case, we have confidence that the transport channel could not be hijacked, and be unnoticed of such interrupted connection. However, telecommunications protocols ignore transmission micro-outages or even signal power drops due to communication interferences.

Nowadays, it is possible to tap any type of communication, including fiber optic networks, interrupting the connection for a short period of time and causing a damage in the fiber optic cable or causing a no significant decrease signal quality so that it will be necessary the use of special equipment to detect the network tap. There are some wireless methods such as evanescent coupling or optic dispersion [11].

Consequently, in order to avoid the possible loss of connection continuity of the original actors, it is necessary that the communication system carries out constant verifications and controls that such system is not being intercepted or hijacked by other devices.

6 Conclusion

The following paper presents the different stages that makes it necessary to develop an authentication model that takes into account these principal factors:

- It must be a two-way method and involves people, communication systems, network connections, and devices.
- The authentication process must not only take place at the beginning of communication but also ongoing verifications should also take place in a continuous way.

The aspects developed in this paper present the major difficulties and some aspects regarding scenarios, different examples and several components involved over the different authentication models. It also shows that a deeper analysis must be carried out in order to develop a detailed model or authentication outline to be used for different types of devices according to their use.

Additionally, different phases have been identified such as authentication and continuity, and their related alert/incident management procedures, so that the user is aware that system's unauthorized access events have occurred or the system can perform some actions in case that some suspicious activity is detected. According to this, perhaps it is necessary to develop artificial intelligence systems associated to the authentication process. But this discussion will be managed in a further analysis.

The market is focused on the development of independent but interconnected management devices, in order to use them for different needs, some of them related directly to the human being. However, this type of needs are growing faster than the security systems when using these particular devices, implying the need of a solution. This solution must take into account the variety of components of verification both for people and devices, in order to design appropriate authentication protocols for dealing with these major difficulties.

Finally, this paper could be taken as a start on an original proposal for a more specific continuous authentication model.

References

[1] The University of Tokyo – Department of Biomedical Engineering. Artificial heart – Available at: http://www.bme.gr.jp/Research_info_E/AH.html, last accessed April 10 2017.

[2] CES – Consumer Technology Association – Self Driving Technology. Available at: http://www.ces.tech/Show-Floor/Marketplaces/Self-Driving-Technology, last accessed April 10 2017.

[3] Olufemi Sunday Adeoye, A Survey of Emerging Biometric Technologies - Department of Computer Science University of Uyo, International Journal of Computer Applications (0975 – 8887) Volume 9– No.10, November 2010 . Available at: https://pdfs.semanticscholar.org/2c6c/4f84046be0a9b317f398bf1783e32e5ad771.pdf, last accessed April 10 2017.

[4] John Daugman. How Iris Recognition Works. IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004. Available at: https://www.cl.cam.ac.uk/~jgd1000/csvt.pdf, last accessed April 10 2017.

[5] Antonio Iula, Alessandro, Stuart Savoia, Giosue Caliano – An ultrasound technique for 3D palmprint extraction, Sensors and Actuators A: Physical Volume 212, 1 June 2014, Pages 18–24. Available at: http://www.sciencedirect.com/science/article/pii/S0924424714001162 , last accessed April 10 2017.

[6] A Winda, W R E Byan, Sofyan, Armansyah, D L Zariantin and B G Josep - Motorcycle Start-stop System based on Intelligent Biometric Voice Recognition OP Conf. Series: Materials Science and Engineering 187(2017) 0120 39 doi:10.1088/1757-899X/187/1/012039. Available at: http://iopscience.iop.org/1757-899X/187/1/012039, last accessed April 10 2017.

[7] Joshua Wheeler, Brigitte Richardson, Scott Amman, Ranjani Rangarajan - Systems Engineering Approach for Voice Recognition in the Car - SAE International Journal of Passenger Cars - Electronic and Electrical Systems 10(1) · March 2017 - DOI: 10.4271/2017-01-1599

[8] Fumihiro Adachi, Ryosuke Isotani, Ken Hanazawa - Voice recognition system, voice recognition method, and program for voice recognition . Patent: US8639507B2 · License: USPTO TOS Date of Patent: Jan 28, 2014. . Available at: https://www.google.com/patents/US8639507, last accessed April 10 2017.

[9] P.Inbavalli , G.Nandhini, Body Odor as a Biometric Authentication - / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6270-6274 Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.661.6164&rep=rep1&type=pdf , last accessed April 10 2017.

[10] MIT –Massachusetts Institute of Technology – d'Arbeloff Laboratory for Information Systems and Technology. Available at: http://darbeloff-lab.scripts.mit.edu/darbeloff-lab/?page_id=296, last accessed April 10 2017.

[11] MillerSandra Kay, Fiber optic networks vulnerable to attack - Revista Information Security – November 2006. Available at: http://searchsecurity.techtarget.com/news/1230106/Fiber-optic-networks-vulnerable-to-attack, last accessed April 10 2017.