Technologies used to provide airport security

Law, Security

There is no doubt that airport security has been changed significantly during the past decades. After the incident of Cubana Flight 455 on October 6, 1976 (world’s first terrorist attack while in flight) security screening at the airport has been getting tighter and tighter. As a result, the airport security today has become more invasive and time-consuming for the passengers. In the meantime, airport security mechanisms have become pretty costly to the airport from an economic point of view.

It is necessary to make sure that the right people will board to the right plane at the right time. For that to happen, information regarding the passenger’s identity is crossed checked multiple times while they are en route to their plane. For example, their passport is checked at luggage drop-off, before they board their plane and sometimes even at the security screening of hand baggage that use X-ray scanners. All the previous procedures comprise an inevitable trade-off between integrity and availability in airport security.

Moreover, certain sharp objects and liquid substances that can be used to initiate an airplane hijack have been banned and passengers cannot carry them in flight. Thus, all travelers are required to pass through body scanners. Additionally, at random intervals travelers are checked for traces of explosives or drugs by using Ion Scanners. Luggage are no exception to this rule either, they get through a security screening and a full passenger bag match is being demonstrated on a daily basis. Furthermore, in order to make airport security even stronger, access is restricted even to the members of the personnel. All individuals employed at the airport require a special card that will grant them access to certain areas depending on their job. For

example, an employee that works at the duty free shops has no business entering baggage handling areas. In other words, his level of access is limited only to his workplace (Principle of least privilege).

Another technology that has been already used extensively for years are security cameras that protect the perimeter of the airport twenty four hours a day. Moreover, the world’s airport authorities are planning to add thermal security cameras that will be protecting airport employees, passengers, planes and equipment.

In addition, in this ever-expanding era of technology, new security methods have been added to airport security. One of them is the technology of facial recognition. It has already been tested at Orlando airport and the U. S. Customs and Border Protection claim that the technology is 99% accurate and helps to thwart terrorism. However, while its effectiveness is still assessed, Bio-metric images that hold travelers’ unique human characteristics are being temporarily stored for 14 days which may harm personal privacy.

However, confidentiality, integrity and availability requirements differ from organization to organization. For example, a private medical doctor may be prepared to sacrifice availability in order to protect the confidentiality of medical records. Each patient’s data needs to be visible only to the doctor that is associated with the patient. Medical records that are stored in computer systems may be a targeted by unauthorized access. To combat this treat, a very important component of protecting information confidentiality is encryption. Encryption ensures that only the right people

who have access to the key that decrypts the data can read the information. If unencrypted data are leaked electronically by malware or shared intentionally (by bribery) to a third party they can severely impact the patient. For example, if an insurance company that insures people against a certain illness gets access to the medical history of each person then the company can selectively deny insurance to people that are in high risk according to their data.

On the other hand, an online bookstore’s priority is the availability of its website in order to protect its revenue. To make this happen, it may increase the geographical distribution of its content delivery systems and servers. However, this will increase the attack surface significantly. As a result, the confidentiality of data that is held in the system is at a greater risk. For example a denial of service (DoS) attack that will flood the servers with illegitimate traffic will cripple the system’s availability. By making the online bookstore’s website unavailable, clients may turn to competitors and may never come back. The average DoS attack cost for businesses rises to over $2. 5 million.

In contrast to the previous example, a banking system may be prepared to sacrifice availability in order to protect the integrity of its financial data. Imagine what can happen if an attacker gains access to a banking system and maliciously alter transactions and account numbers so that he can gain profit. That would be a failure of integrity, because in this case important financial data have been altered without authorization. Another example of a failure of integrity is when someone tries to connect to the bank’s website

and a malicious attacker between the victim and the website redirects the traffic to a different website which is not genuine. This attack is also known as the Man in the Middle attack (MiTM).

Apart from the CIA triad (confidentiality, integrity and availability), other important factors in security are sustainability and resilience. Sustainability implies continuity, it means that the system that we have built is able to last or continue for a long time.