4.3.4 Securability

Return to Non-Functional Requirements

About

Security is not a single “thing” that can be added to a system. To be truly secure, the entire End-to-End Solution (E2ES) needs to be secure and needs to be considered during the entire System Lifecycle. As shown in Figure 1, a layered approach is used to help isolate the security needs. Each layer represents a portion of the Information Technology (IT) stack, including the people who use and have access to the IT stack.

Figure 1: The layers of security.
Table 1: Definitions for layers of security

Layer	Description
Physical Security	The physical security is concerned with preventing physical harm to the Computing Platform (e.g., theft, fire, flooding, etc.), as well as, preventing access to the physical platform via “back doors” thereby allowing breaches by potentially malicious actors (e.g., using pluggable USB drives, adding wire sniffers to the network, or the internal threat posed by employees with access). • **Note:** Even though the role of Phsyical Security has somewhat diminished with the acceptance of the Zero Trust Security Model and Zero Trust Architecture (ZTA), it still plays a key role as the first line of defense, but by itself, it is not enough.NIST: SP 800-207: Zero Trust Architecture (ZTA) • Zero Trust Security Model • Zero Trust Architecture (ZTA) • The Onion Router (Tor)
Data Security	Data security ensures that Data-at-Rest, Data-in-Motion, or Data-in-Use remains intact (i.e., completeness, accuracy and consistency). For example, allowing incomplete data to be stored (i.e., date of a transaction, or *authorized by* fields). Roundoff Error can also affect the accuracy of the data. Modifying a bank account balance introduces inconsistencies that can be detected. • **Note:** Formalization of Zero Trust Security Model and Zero Trust Architecture (ZTA) has set a goal of: *“preventing unauthorized access to data and services coupled with making the access control enforcement as granular as possible. ”*NIST: SP 800-207: Zero Trust Architecture (ZTA) • **Note:** Another way to achieve data security while the data is in motion is to use The Onion Router (Tor) which was designed by the U.S. Navy to protect sensitive documents https://whatis.techtarget.com/definition/TOR-third-generation-onion-routing. • Zero Trust Security Model • Zero Trust Architecture (ZTA) • The Onion Router (Tor)

Layer	Description
Network Security	Network security issues are generally the result of unaddressed network vulnerabilities. There are three main network categories for vulnerabilities: software, hardware, or organizational processes. Software and hardware that are not kept current are subject to malicious attacks by merely exploiting known vulnerabilities. Another issue for networks are social engineering attacks where people violate hardware and software protection policy and procedures to compromise the data. The first line of defense for networks is the use of a Hardware Firewall, which predominately protects the Network Nodes inside a Local Area Network (LAN) from external Nodes on the Internet. Another common tool is the use of Networking Access Control Lists (ACLs). • Hardware Firewall • Access Control List (ACL) • Hypertext Transport Protocol Secure (HTTPS) • Secure Sockets Layer (SSL) • Transport layer security (TLS)

Platform Security	Platform security involves an attack on a Computing Platform by the introduction of malicious software, the modification of access controls or configuration data, or having incorrectly configured settings (i.e., Software Firewall, Access Control List (ACL), Full-Disk Encryption (FDE)). Many platforms can require authorization of peripheral functions such as geo-location services, Bluetooth, TCP/IP networks, radio networks, and segmented portions of the disk storage such as photos.
	• Software Firewall
	• Access Control List (ACL)
	• Full-Disk Encryption (FDE)
	• Full Memory Encryption (FME)
	• Authorization of Peripheral Device such as:
	  ◦ Geolocation services,
	  ◦ Bluetooth
	  ◦ Transmission Control Protocol (TCP) networks
	  ◦ Wireless Network
	  ◦ segmented portions of the disk storage

Layer	Description
Application Security	Application Security features include authentication of users using multi-factor authentication such as user id and Password, asking additional questions only the user knows the answer to, use of a One-Time PIN (OTP) to a known device, a fingerprint or face recognition. Application Security also includes authorization that maps the user's identity with a list of applications the user can access and even the privileges the user has within the application (read/write/delete, etc). Sometimes an application can encrypt information as it moves between the components of the system (CPU, Memory, Disk, network, etc.). Another key aspect is the secure logging of activities occurring within an application (e.g., the user granted access, the user deletes information, user updates information, etc.) • Authentication • Access Control • Multifactor Authentication (MFA) • One-Time PIN (OTP) • Two-Factor Authentication (2FA) • N-Tier Architecture
Culture Security	One of the biggest threats to any system or program is the internal threat caused by inadvertent or overt actions taken by the people within the organization. To overcome these threats, there needs to be Cultural Security (also known as cybersecurity) that seeks to change the mindset of the authorized users. Some basic examples are not using `password` as a Password, not writing the passwords on paper, having a separate password for every person, changing the password every so many days, keeping ACLs up to date, and reflecting on the current roles and responsibilities of the users. Sometimes, it comes down to just observing the behavior of others[1)] • Non-Disclosure Agreement (NDA) • Data Loss Prevention (DLP) • Disaster Recovery Plan (DRP) • Business impact Analysis (BIA)

ISO/IEC 25010 defines Security as the degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization. This characteristic is composed of the following sub-characteristics[2)]:

- 4.3.4.1 Confidentiality
- 4.3.4.2 Data Integrity
- 4.3.4.3 Non-Repudiation
- 4.3.4.4 Authenticity
- 4.3.4.5 Accountability

See DIDO Specifics

Return to Top

To be added/expanded in future revisions of the DIDO RA

1)

Cyber Security Culture in organizations, European Union Agency for Network and Information Security (ENISA), November 2017, Accessed on 13 August 2020, https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

2)

ISO25000 Software and Data Quality ISO/IEC 25010, 2011, Accessed 13 August 2020, https://www.iso.org/obp/ui/#iso:std:iso-iec:25010:ed-1:v1:en