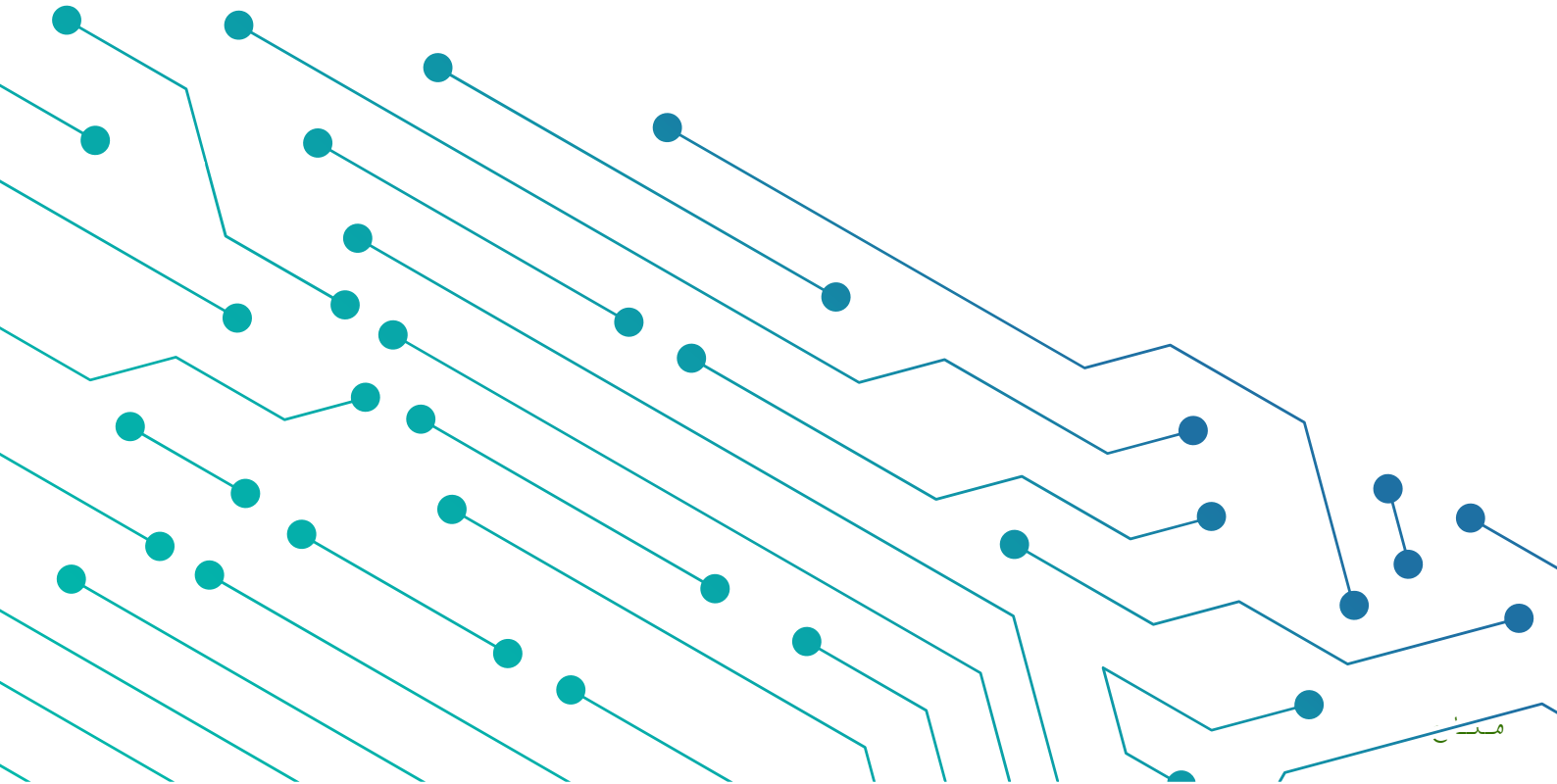
الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Draft

General Principles of Secure-by-Design

(SBD – 1: 2020)

Sharing Indicator: White
Document Classification: Unclassified



In the Name of Allah,
The Most Gracious,
The Most Merciful

Traffic Light Protocol (TLP)

This marking protocol is widely used around the world. It has four colors (traffic lights):

Red - Personal, Confidential and for Intended Recipient only

The recipient has no rights to share information classified in red with any person outside the defined range of recipients either inside or outside the organization.

Amber - Restricted Sharing

The recipient may share information classified in amber only with intended recipients inside the organization and with recipients who are required to take action related to the shared information.

Green - Sharing within the Same Community

The recipient may share information classified in green with other recipients inside the organization or outside it within the same sector or related to the organization. However, it is not allowed to exchange or publish this information on public channels.

White - No Restrictions

Table of Contents

Executive Summary

The expansion of the use of technology opens new horizons for cyber threats, which require flexibility and keeping pace with cyberspace trends, in addition to actively dealing with the technological developments in order to mitigate such threats.

Therefore, the Kingdom is working on adopting a proactive and strategic approach that takes cyber threats into consideration. This approach covers the implementation of new initiatives, IT projects and the management of their changes.

From this perspective, the National Cybersecurity Authority (hereinafter referred to as "NCA") worked on the secure-by-design initiative that aims at spreading the best practices in this regard. Amongst the efforts included in this initiative, this document was developed to offer a set of secure-by-design general principles to guide the stakeholders in terms of key practices in cybersecurity. The methodology used to develop this document consisted of the following key steps:

- Analysis of international experiences in this field
- Inputs and opinions of cybersecurity specialists
- Study of the best secure-by-design international practices

A compressive design approach was used to develop the secure-by-design principles (which is depicted in figure 1 below). It is based on three layers:

- First: a foundation layer that is applicable for all kinds of services and technologies,
- Second: a domain specific layer for certain domains similar in nature,
- Third: an application specific layer for specific kind of applications and solutions.

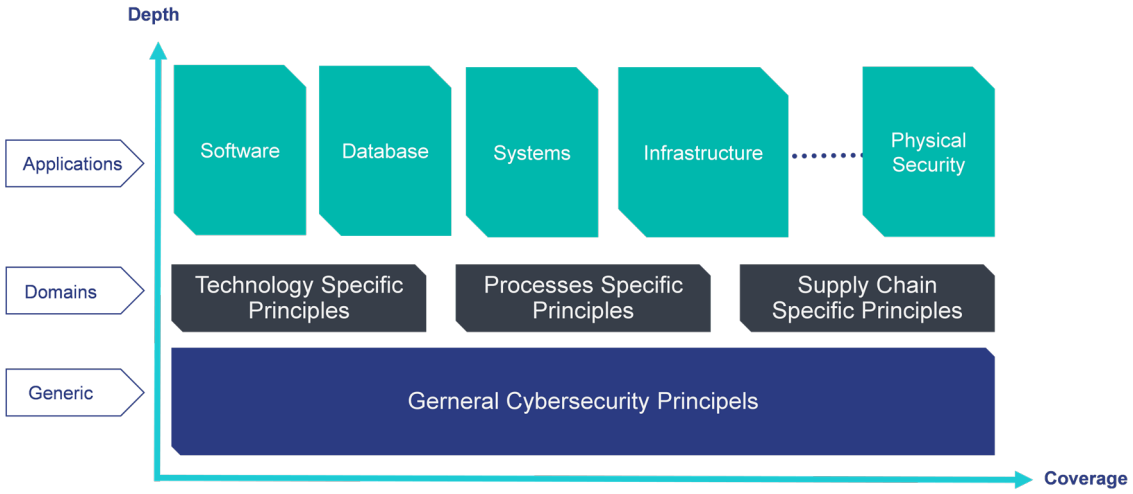


Figure 1. Secure-by-Design Approach.

Accordingly, eight principles of the key secure-by-design practices were identified:

1. Least Privileges
2. Need to Know
3. Segregation of Duties
4. Avoid Security by Obscurity
5. Defense in Depth
6. Zero Trust
7. Secure Defaults
8. Attack Surface Reduction

Introduction

The existence of a national, integrated and secured digital infrastructure is one of the most important factors for development and prosperity. In fact, such infrastructure requires that information can flow, is secure, and is integrated between the systems. It is crucial for the Kingdom's cybersecurity to be maintained and enhanced to protect the Kingdom's vital interests, national security, critical infrastructures, priority sectors and governmental services and activities.

The expansion of technology usage opens new horizons for security vulnerabilities and cyber threats which requires enhancing cybersecurity to protect networks, IT systems, operational technologies systems and components, including devices, software and protection of provided services and its data from any hacking, disruption, unauthorized amendment, login, use or exploitation. Furthermore, this aims at enhancing the security of the technical integration between the governmental services in order to support the digital economy.

Processing the cybersecurity aspects after developing the systems increases cost, makes implementation harder and requires doubled efforts to ensure, test and launch the systems not to mention the risks resulting from the solution's inefficiency in controlling and testing vulnerabilities during operation and risks resulting from not updating the systems rapidly and effectively.

The Kingdom is working on adopting a proactive approach to enhance the cybersecurity aspects in the systems, devices and services, starting from design to production to operation, and lastly, destruction, in order to achieve technical standards that ensure the existence of high security and quality systems, devices and services. Thus, NCA worked on the secure-by-design initiative that aims to take the cybersecurity aspects into consideration in all phases of development, as well as examining any system –including all its components –regarding cyberattack vulnerability, which requires building adequate defenses at all phases.

This document presents a set of secure-by-design general principles, which aim to clarify and spread the key practices in this aspect, and which may be adopted on a wide scale, while presenting each principle with a relevant example. Through this document, NCA looks forward to launching the secure-by-design initiative, which will contribute to achieving a safe and reliable Saudi cyberspace

Methodology

The secure-by-design principles were built within a comprehensive methodology and key steps, starting with studying the main local and international cyber technical risks and developing a comprehensive and complementary framework that covers all phases of offering technical solutions. Furthermore, Learning was taken from the best international expertise and practices that meet the Kingdom's needs. Input and opinions were taken from cybersecurity specialists on the national level in order to formulate a clear and comprehensive methodology and to develop a set of general principles.

These principles directly help in achieving the following:

- Enhancing cyber resilience.
- Reducing the cyberattack scope.
- Integrating the cybersecurity controls with the main functions of the technical solutions.

These principles are aligned with NCA's other publications. This document represents a starting point for the secure-by-design initiatives with the determined scope and the specific nature.

Document Scope

This document presents a set of secure-by-design guidelines for awareness purposes. NCA encourages all authorities and sectors in the Kingdom, regardless of the nature of their work, to adopt these principles in order to prepare, develop and operate IT projects and operational technologies, and to mitigate cyber risks in their business, systems and data.

General Principals

1 Least Privileges

Restricting the users' access[1] within the scope of their work and specialty in order to implement only the functions entrusted to them.

This principle depends on granting the users the minimal necessary access to complete their assigned functions. This principle applies to all levels in the system including users, programs, networks, applications and all different IT aspects.

In order to implement this principle, the business processes and requirements must be analyzed, including the analysis and classification of relevant data, resulting in restricting the users' access as per their roles and responsibilities to the minimum level required to perform their functions.

This principle prevents the possibility of accessing the systems or the data that are unnecessary for the user, thereby reducing risks related to data leakage or illegitimate actions and downsizing the possible scope of attack.

Example

An HR employee may need to have access to read and edit the payroll database, however, his/her functions do not require access to the customers' database; at the same time, the functions of the sales employee only require access to the customer's database (without the need to access the payroll database).

[1] In this document, "users" are referred to as actual people or UserAccounts, systems and programs.

2 Need to Know

Limiting access to information to authorized users the nature of whose work requires accessing such information.[2]

This principle relies on limiting the access to information to authorized users, the nature of whose work requires this access. Users are not allowed complete access to all information.

This principle may be applied by different means such as applying an effective segregation of systems, controlling access to specific records, and setting technical controls such as determining the periods of times in which information access is allowed.

This principle aims at putting an end to unauthorized access without affecting the business's performance. It also aims to block access to restricted information through limiting access to the minimum possible number of users.

Example

Granting Department Managers access to necessary information on employees that are under their management only, in order to implement their administrative functions. Personal information about employees may not be shared with the direct manager unless required.

2 The principle "Least Privileges" means what the user can implement in terms of activities, whereas this principle means the data that the user can access.

3 Segregation of Duties

The participation of more than one person to implement a specific operation during different phases.

The segregation of functions or the segregation of duties is a principle that aims to divide a function into multiple phases to implement a specific operation by ensuring the existence of more than one person to complete these phases and with the appropriate access rights.

This principle is achieved by segregating sensitive functions[3] to several steps that are all considered necessary to complete the function and assign each step to one person or different team.

The implementation of this principle reduces individual mistakes of sensitive functions and prevents any person from violating the cybersecurity controls on their own.

Example

Change requests must be adopted by more than one person. For example, firewall regulations must be implemented by one person and approved by another. Similarly, requests and payrolls are submitted by one person and approved by another.

[3] Example of authorization functions as well as audit and asset immunity functions.

4 Avoid Security by Obscurity

Avoid relying on the obscurity of the systems' contents and design, and hiding their details as a key method of securing the systems.

Obscurity of the systems' contents and design as a means to secure the systems gives a wrong impression, since it is possible to know the systems' contents and design through different means. The principle of security by obscurity can be used as an additional means of defense. However, the system's security must not depend on the confidentiality of its design or contents.

Security by obscurity is a principle that contradicts the secure-by-design principle. The systems' design must be carried out by secure controls without using the obscurity of their contents or hiding their internal details as a key method to secure them.

This principle aims to protect the systems in case of an information leakage regarding the systems' contents and design, by not relying on obscurity as a key method for security.

Example

Avoid hiding passwords of accounts in text files stored in a hidden folder, or changing the name of the folder of sensitive applications (e.g. from "admin" to "admin2"), and using internally developed encryption mechanisms.

5 Defense in Depth

Setting several layers of security controls as defense mechanisms.

A concept for information assurance where several layers of security controls are applied as a defense series meaning if one mechanism fails, there will be another to back it up.

Among the basics of the implementation of this principle are: the use of multithread mechanisms such as firewalls, detection systems, prevention of infiltration, data encryption and auditing and review systems, as well as setting physical and procedural security mechanisms.

This principle aims to increase the systems' security by mitigating vulnerabilities, patching security vulnerabilities, increasing the difficulty of attacks, and improving the ability of detecting and responding to attacks.

Example

Obtaining the necessary approvals for physical access of servers and logging in by using two factor authentication technologies and activating events records and surveillance cameras, in addition to encrypting data (during transmission and storage) and using data leakage prevention technologies.

6 Zero Trust

Verifying all users and their user rights before granting access.

All trusted parties, including users, third parties and others, may pose a risk to the systems. Therefore, each user, even reliable ones, must be verified when using any service or system.

In terms of the zero-trust concept, users and their rights must be verified, including the internal users and third parties, in addition to activating follow-up and surveillance mechanisms when using the services and systems.

Among the major benefits of implementation of this principle is knowing the systems' users and analyzing the data that detect some operational vulnerabilities, in addition to mitigating the cybersecurity risks relevant to third parties.

Example

Data leakage is possible for any person with access to the network. In order to avoid such leakage, every identity and operation must be verified and registered while applying other adequate mechanisms, such as encryption.

7 Secure Defaults

Designing products and services with default configuration settings that meet the best security practices.

This principle states that systems must be designed in a way that their default configuration settings are secure without the need for any action to be taken by the user in order to set the system securely.

The concept of this principle lies in activating the security advantages in the system's settings by default and deactivating the insecure settings, while balancing the need to provide an easy user experience.

This principle aims to raise the security level when using products and services and reduce risks related to the lack of knowledge by the user regarding the best security practices or neglecting their application.

Example

Activating two factor authentication when logging into the system, and not configuring the systems by default authentication information (e.g. the name of the user and the password).

8 Attack Surface Reduction

Decreasing the exposure of what must be protected (i.e. systems, devices and applications), and reducing direct attacks on them.

The attack surface includes any access points to the systems that allow adversaries to exploit (including the components of devices, applications and others). This scope expands with the increase of the complexity of systems and multiple benefits making it more vulnerable to security attacks, which implies the importance of simplicity in designing any system.

Attack surface may be reduced by decreasing the unnecessary complexities in the systems such as, reducing the system's source code and relevant external systems, as well as deactivating unnecessary features and services.

This principle aims to reduce attack points (Attack Vector) that the hacker can detect and try to exploit.

Example

Disabling unnecessary ports in the systems, reducing the users' authorizations and removing unused applications and services.