

Healthcare Computer Network

Requirements Document

Purpose

This document defines the computer network requirements to ensure the confidentiality, integrity and availability of sensitive healthcare data. Data exchange is permitted only between devices in the same network zone or across zones connected by explicitly defined directional Security Enforcement Rules (SERs), specifying authorized communication and permitted data sensitivity levels.

This document provides a foundation for formal modelling and verification of healthcare network security, including dynamic incident response.

Scope

The document specifies requirements related to:

- Logical structure of the computer network;
- Data exchange between network elements;
- Authorization relationships between network zones;
- Operational behavior under security enforcement during cyber incidents.

The following is explicitly out of scope of the document:

- Human behaviour;
- Physical hardware characteristics;
- Implementation of network devices;
- Cryptographic algorithms and key management.

Data threat context

Integrity

- Ransomware attacks targeting critical systems and database
- Sensitive data modified or deleted
- Security goal – ensure high sensitivity data exchange is allowed only along authorized paths; network parts are isolated in case of compromise.

Confidentiality

- Data exfiltration attacks
- Sensitive data being exposed
- Security goal – prevent unauthorised access to high-sensitivity network parts.

Multi-zone threat

- Multiple zones compromised at the same time
- Security goal – define the isolation and recovery procedures to handle overlapping compromises while maintaining critical operations.

Definitions

Data – Information exchanged within the network between devices, classified by sensitivity

Device – An abstract network entity that can send or receive data

Zone – A network segment defined as a set of devices with identical trust level and data access constraints

Security enforcement rule (SER) – A directional authorization of a hop defining the maximum permitted data sensitivity level for data exchange

Hop – A directed connection between two zones authorized by a security enforcement rule

Path – An ordered sequence of hops connecting zones

Static structural requirements

Data sensitivity

R1. All data exchanged in the network shall be classified by its confidentiality level:

- Public
- Internal
- Confidential
- Restricted

R2. Data sensitivity levels are totally ordered:

$$\text{Public} < \text{Internal} < \text{Confidential} < \text{Restricted}$$

Note: *The ordering defines a security lattice used to constrain permitted data flows.*

Zone trust level

R3. Zone trust level is categorized as:

- Public (PZ)
- Public Access Zone (PAZ)
- Operations (OZ)
- Restricted (RZ), subdivided into:
 - Administration (AZ)
 - Critical (CZ))

R4. Trust levels are totally ordered:

$$\text{PZ} < \text{PAZ} < \text{OZ} < \text{RZ} (\text{AZ} = \text{CZ})$$

Note: *For the static security analysis, AZ and CZ are considered equivalent in the trust hierarchy. Distinction between AZ and CZ is relevant in dynamic network reconfiguration.*

Zones

R5. The network shall maintain the following zones:

- Guest
- DMZ
- Enterprise
- Lab
- Core
- Database

- Backup
- Clinical
- IoMT

R6. Each zone shall have a trust level assigned (according to R3):

R6.1. Guest zone shall have a trust level PZ

R6.2. DMZ zone shall have a trust level PAZ

R6.3. Enterprise zone shall have a trust level OZ

R6.4. Lab zone shall have a trust level OZ

R6.5. Core zone shall have a trust level AZ

R6.6. Database zone shall have a trust level AZ

R6.7. Backup zone shall have a trust level CZ

R6.8. Clinical zone shall have a trust level CZ

R6.9. IoMT zone shall have a trust level CZ

Devices

R7. The network shall maintain a finite, non-empty set of devices.

R8. Every device shall belong to exactly one zone.

Security Enforcement Rules

R9. The network shall maintain a finite set of Security Enforcement Rules defined as directional authorization relations over zones.

R10. Any data exchange not explicitly permitted by the security enforcement rule is denied (deny-by-default policy).

R11. Security enforcement rules are directional.

R12. Each security enforcement rule shall be defined by the following attributes:

R12.1. Source zone

R12.2. Destination zone

R12.3. Maximum permitted data sensitivity level

R13. The following security enforcement rules shall be implemented:

- R13.1.** Guest → DMZ : Public
- R13.2.** DMZ → Guest : Public
- R13.3.** DMZ → Enterprise : Internal
- R13.4.** Enterprise → DMZ: Public
- R13.5.** Enterprise → Core : Confidential
- R13.6.** Lab → Core : Confidential
- R13.7.** Core → Enterprise : Confidential
- R13.8.** Core → Lab : Confidential
- R13.9.** Core → Database : Restricted
- R13.10.** Core → Clinical : Restricted
- R13.11.** Database → Core : Restricted
- R13.12.** Database → Backup : Restricted
- R13.13.** Backup → Database : Restricted
- R13.14.** Backup → Clinical: Restricted
- R13.15.** Clinical → Core : Restricted
- R13.16.** Clinical → Backup : Restricted
- R13.17.** Clinical → IoMT : Restricted
- R13.18.** IoMT → Clinical : Restricted

Paths

- R14.** A path is a non-empty finite sequence of Security Enforcement Rules such that consecutive rules are composable (destination of the first SER equals source of the next SER).
- R15.** The set of valid paths is derived from the Security Enforcement Rule relation.
- R16.** Each security enforcement rule defined in R13 shall constitute as a valid single-hop path with maximum data sensitivity level equal to the SER's maximum data sensitivity level.
- R17.** Each zone shall appear no more than once within a single path.
- R18.** The maximum data sensitivity level allowed for a path shall be limited to the lowest maximum data sensitivity level permitted by any of the included security enforcement rules.
- R19.** In addition to single-hop paths defined in R13, the following paths shall be implemented:

R19.1. Enterprise shall be reachable from Guest.

R19.2. Guest shall be reachable from Enterprise.

R19.3. Database shall be reachable from Enterprise.

R19.4. Database shall be reachable from Lab.

R19.5. Enterprise shall be reachable from Database.

R19.6. Lab shall be reachable from Database.

R19.7. Clinical shall be reachable from Database.

R19.8. Database shall be reachable from Clinical.

R19.9. IoMT shall be reachable from Core.

R19.10. Core shall be reachable from IoMT.

R19.11. Backup shall be reachable from IoMT.

R19.12. IoMT shall be reachable from Backup.

Critical Paths

R20. The network shall maintain a finite set of critical paths which availability shall be ensured with defined data sensitivity level under all network operational modes defined in this document.

R21. The following critical paths shall be ensured:

R21.1. Connection between clinical and medical devices

R21.1.1. Clinical → IoMT (R13.17)

R21.1.2. IoMT → Clinical (R13.18)

R21.2. Connection between clinical devices and data administration systems (mode dependent):

R21.2.1. Usual network mode:

R21.2.1.1. Clinical → Database (R19.8)

R21.2.1.2. Database → Clinical (R19.7)

R21.2.2. Reconfiguration mode:

R21.2.2.1. Clinical → Backup (R13.16)

R21.2.2.2. Backup → Clinical (R13.14)

Dynamic behavioural requirements

Monitoring

R22. The network shall maintain a continuous monitoring of the devices and zones.

R23. Each device shall be classified by the monitoring system as:

- Secure
- Compromised

R24. Each zone shall be classified by the monitoring system as:

- Secure
- Isolated
- Reconnecting

R25. The network shall be classified by the monitoring system as:

- Secure
- Operational
- Reconfiguring
- Recovering

R26. The initial classification of each device is Secure.

R27. The initial classification of each zone is Secure.

R28. The initial classification of the network is Secure.

R29. Upon detection of a cybersecurity incident affecting a device, the monitoring system shall classify the device as Compromised.

R30. Zone classification shall satisfy the following consistency requirements:

R30.1. Zone shall be classified as Secure if and only if:

R30.1.1. All devices in that zone are classified as Secure

R30.1.2. All security enforcement rules involving that zone are established

R30.2. Zone shall be classified as Isolated if and only if:

R30.2.1. At least one device in that zone is classified as Compromised

R30.2.2. Isolation procedures (R34-R36) have been applied.

R30.3. Zone shall be classified as Reconnecting if and only if:

R30.3.1. All devices in that zone are classified as Secure

R30.3.2. At least one security enforcement rule involving that zone is not established.

R30.4. The conditions specified in R30.1, R30.2, and R30.3 shall be maintained as mutually exclusive and collectively exhaustive by construction.

R31. Network classification shall satisfy the following consistency requirements:

R31.1. The network shall be classified as Secure if and only if all zones in the network are classified as Secure.

R31.2. The network shall be classified as Operational if and only if:

R31.2.1. At least one zone is classified as Isolated

R31.2.2. All zones not classified as Secure or Reconnecting have zone trust level equal to PZ, PAZ, or OZ.

R31.3. The network shall be classified as Reconfiguring if and only if at least one zone with trust level RZ (AZ or CZ) is classified as Isolated.

R31.4. The network shall be classified as Recovering if and only if:

R31.4.1. At least one zone is classified as Reconnecting

R31.4.2. No zones are classified as Isolated.

R31.4.3. All other zones classified as Secure

R31.5. The conditions specified in R31.1, R31.2, R31.3, and R31.4 shall be maintained as mutually exclusive and collectively exhaustive by construction.

Cybersecurity Incident Response

R32. Backup zone shall operate in one of two modes: Idle and Reconfiguration.

R33. When network is classified as:

R33.1. Reconfiguring – the Backup zone shall operate in Reconfiguration mode.

R33.2. Secure, Operational, or Recovering – Backup zone shall operate in Idle mode.

R34. Upon detection of a cybersecurity incident in zone with trust level PZ, PAZ, or OZ, the network shall isolate the compromised zone by denying all data exchange between the compromised zone and any other zone.

R35. Upon detection of a cybersecurity incident in zone with trust level AZ, the network shall:

R35.1. Deny all data exchange with zones with trust level PZ and PAZ.

R35.2 Deny all data exchange above Internal sensitivity level between the compromised zone and zones with trust level OZ.

R35.3. Maintain all SERs between the compromised AZ zone and all other AZ zones.

R35.4. Deny all SERs from all AZ zones to all CZ zones.

R35.5. Deny all SERs from all CZ zones to all AZ zones.

R35.6. Transition Backup zone to Reconfiguration mode.

R36. Upon detection of a cybersecurity incident in zone with trust level CZ, the network shall:

R36.1. Deny all data exchange with zones with trust level PZ, PAZ, OZ, and AZ.

R36.2 Maintain all SERs between compromised zone and all other CZ zones.

R36.3. Transition Backup zone to Reconfiguration mode.

R37. Compromised zone isolation shall remain until all devices in the zone are classified as Secure by the monitoring system.

R38. Backup zone shall transition from Reconfiguration mode to Idle mode when all AZ and CZ zones are classified as Secure and the network is classified as Recovering.

R39. Upon remediation and validation of all compromised devices in a zone (all devices classified as Secure), the zone shall transit back to Secure mode and resume normal operations.

Threat-to-Requirements Mapping

Ransomware attack threat is mitigated by requirements:

- R9 to R21 (containment through authorized paths)
- R22 to R31 (detection through continuous monitoring)
- R32 to R39 (response through isolation and recovery).

Data exfiltration attack threat is mitigated by requirements:

- R1 and R2 (data classification)
- R9 to R21 (prevention through access control)
- R22 to R31 (detection through continuous monitoring).

Multi-zone compromise threat is mitigated by requirements:

- R22 to R31 (detection through continuous monitoring)
- R32 to R39 (state management, isolation, and recovery procedures).

Formal verification properties

Static security properties

SP1. Confidentiality: Restricted data shall never reach zones with trust level PZ, PAZ, or OZ.

SP2. Critical Availability: All critical paths defined in R21 shall exist as valid paths in the network.

SP3. Architectural Integrity: Every hop in every path shall connect zones whose trust levels are either equal or differ by at most one level in total ordering.

Dynamic security properties

DP1. Dynamic Reconfiguration: Upon detection of compromise in any zone with trust level AZ or CZ, the network shall eventually transition to Reconfiguring mode.

DP2. Critical Availability: All critical paths defined in R21 shall exist as valid paths in the network at all times.

DP3. Backup Adaptiveness: The Backup zone connectivity shall adapt to network operational mode:

- Idle mode – connected to AZ, disconnected from CZ;
- Reconfiguration mode – connected to CZ, disconnected from AZ

as defined in R32, R33, R35, R36, R38, R39.