Healthcare Computer Network

Formal Specification

The resilient healthcare computer network architecture is defined as:

$$\begin{aligned}\mathbf{HCN} = (&\mathbf{Z}, \mathbf{ZL}, \mathbf{D}, \mathbf{S}, \mathbf{inZone}, \mathbf{trustLevel}, \mathbf{SER}, \mathbf{P}, \mathbf{CP},\\ &\mathbf{pathZones}, \mathbf{pathSensitivity}, \mathbf{zoneCompromised},\\ &\mathbf{networkMode}, \mathbf{activeSER}, \mathbf{backupMode})\end{aligned}$$

with the following static components:

- $Z = \{Guest, DMZ, Enterprise, Lab, Core, Database, Backup, Clinical, IoMT\}$
  A finite set of zones;

- $ZL = \{PZ, PAZ, OZ, RZ\}$, where $RZ = \{CZ, RZ\}$

  A finite set of strictly ordered trust levels, where:

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

  We rely on a successor function $Next$ that returns the higher zone, i.e.
  $Next(PZ) = PAZ$, $Next(PAZ) = OZ$, $Next(OZ) = RZ$, $Next(RZ) = RZ$.

- D is an abstract, non-empty finite set of system devices;

- $S = \{Public, Internal, Confidential, Restricted\}$

  A finite set of strictly ordered data sensitivity levels, where:

  $$Public < Internal < Confidential < Restricted;$$

- $inZone : D \to Z$
  A total function that maps each device to its zone;

- $trustLevel : Z \to ZL$
  A total function that maps each zone to its security level;

- $SER \subseteq Z \times Z \times S$
  A finite set of Security Enforcement Rules. Additionally, the named projection functions are defined: $src(p)$ denotes the source zone; $dst(p)$ denotes the destination zone; $mds(p)$ denotes the maximum data senstivity level;

- $P \subseteq seq(SER)$
  A finite set of paths where each $p \in P$ is a sequence of SERs;

- $CP \subseteq P$
  A non-empty finite set of critical paths;

- $pathZones : P \to \wp(Z)$
  where $pathZones(p) = \{src(p[i]) | i \in 1..|p|\} \cup dst(p[|p|])$;

- $pathSensitivity : P \to S$
  where $pathSensitivity(p) = min\{mds(ser) | ser \in p\}$.

Additionally, the specification includes dynamic system components defining the network state:

- $zoneCompromised : Z \rightarrow BOOLEAN$
  A total function mapping each zone to a true/false value, indicating whether zone is compromised;

- $activeSER \subseteq SER$
  A dynamic subset of the currently established Security Enforcement Rules;

- $networkMode \in \{$*Secure, Operational, Reconfiguring, Recovering*$\}$;
  The current network mode;

- $backupMode \in \{$*Idle, Reconfiguration*$\}$;
  The current backup mode.

Static security properties

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

$$\begin{aligned}\textbf{SP1} \triangleq\ & \forall p \in P : \text{pathSensitivity}(p) = \text{Restricted} \Rightarrow \\ & \quad \forall z \in \text{pathZones}(p) : \text{trustLevel}(z) \notin \{\text{PZ}, \text{PAZ}, \text{OZ}\}\end{aligned}$$

noindent **SP2. Critical Path Existence:** *All critical paths defined in R21 shall exist as valid paths in the network.*

$$\begin{aligned}\textbf{SP2} \triangleq\ & (\exists p \in CP : src(p[1]) = \text{Clinical} \land dst(p[|p|]) = \text{IoMT}) \\ & \land (\exists p \in CP : src(p[1]) = \text{IoMT} \land dst(p[|p|]) = \text{Clinical}) \\ & \land (\exists p \in CP : src(p[1]) = \text{Clinical} \land dst(p[|p|]) = \text{Database}) \\ & \land (\exists p \in CP : src(p[1]) = \text{Database} \land dst(p[|p|]) = \text{Clinical})\end{aligned}$$

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

$$\begin{aligned}\textbf{SP3} \triangleq\ & \forall p \in P : \forall i \in \{1, \ldots, |p|\} : \\ & \quad \text{trustLevel}(src(p[i])) = \text{Next}(\text{trustLevel}(dst(p[i]))) \\ & \quad \lor\ \text{trustLevel}(dst(p[i])) = \text{Next}(\text{trustLevel}(src(p[i]))) \\ & \quad \lor\ \text{trustLevel}(src(p[i])) = \text{trustLevel}(dst(p[i]))\end{aligned}$$

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.*

$$\begin{aligned}\textbf{DP1} \triangleq \Box\big((&\exists z \in Z : \text{zoneCompromised}(z) = \text{True} \land\ \text{trustLevel}(z) \in \{\text{AZ}, \text{CZ}\}) \\ &\to \Diamond(\text{networkState} = \text{Reconfiguring})\big)\end{aligned}$$

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

$$\begin{aligned}\textbf{DP2} \triangleq \Box\big(&[\text{Clinical}, \text{IoMT}, \text{Restricted}] \in \text{activeSER} \\ &\land\ [\text{IoMT}, \text{Clinical}, \text{Restricted}] \in \text{activeSER} \\ &\land\ \big(([\text{Clinical}, \text{Core}, \text{Restricted}] \in \text{activeSER} \\ &\qquad \land\ [\text{Core}, \text{Database}, \text{Restricted}] \in \text{activeSER} \\ &\qquad \land\ [\text{Database}, \text{Core}, \text{Restricted}] \in \text{activeSER} \\ &\qquad \land\ [\text{Core}, \text{Clinical}, \text{Restricted}] \in \text{activeSER}) \\ &\quad \lor\ ([\text{Clinical}, \text{Backup}, \text{Restricted}] \in \text{activeSER} \\ &\qquad \land\ [\text{Backup}, \text{Clinical}, \text{Restricted}] \in \text{activeSER})\big)\big)\end{aligned}$$

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

$$\begin{aligned}\textbf{DP3} \triangleq \Box\big(&(\text{backupMode} = \text{Idle} \\ &\quad \to \big([\text{Database}, \text{Backup}, \text{Restricted}] \in \text{activeSER} \\ &\qquad \land\ [\text{Backup}, \text{Database}, \text{Restricted}] \in \text{activeSER} \\ &\qquad \land\ [\text{Clinical}, \text{Backup}, \text{Restricted}] \notin \text{activeSER} \\ &\qquad \land\ [\text{Backup}, \text{Clinical}, \text{Restricted}] \notin \text{activeSER}\big)) \\ &\land\ \big(\text{backupMode} = \text{Reconfiguration} \\ &\quad \to ([\text{Clinical}, \text{Backup}, \text{Restricted}] \in \text{activeSER} \\ &\qquad \land\ [\text{Backup}, \text{Clinical}, \text{Restricted}] \in \text{activeSER} \\ &\qquad \land\ [\text{Database}, \text{Backup}, \text{Restricted}] \notin \text{activeSER} \\ &\qquad \land\ [\text{Backup}, \text{Database}, \text{Restricted}] \notin \text{activeSER})\big)\big)\end{aligned}$$