Table 1: A comprehensive list of meta-level attributes used in CRV

Name	**Description**	**Type**	**Values**	**Default Value**	**Category**
connectionType	Determines the type of a channel	Enumeration	Local, Remote	Remote	Channel
pedigree	Determines how a component has been developed/obtained	Enumeration	InternallyDeveloped, COTS, Sourced	COTS	Component
category	Determines the category of a component	String	-	LOCATION_DEVICE	Component
componentType	Determines the type of a component	Enumeration	Software, Hardware, Human, SwHwHybrid, SwHumanHybrid, HwHumanHybrid, Hybrid	Hybrid	Component
adversariallyTestedForTrojanOrLogicBomb	Determines the level of rigorous testing of a component for adversarial attacks; any value >0 is considered to be secure.	Integer	0-9	0	Component
insideTrustedBoundary	Determines whether a component is inside the trusted boundary in the architecture	Boolean	True, False	False	Component
deviceAuthentication	Determines the level of confidence to authentication mechanism used by a component; any value >0 is considered to be secure.	Integer	0-9	0	Component
inputValidation	Determines the level of confidence to input validation mechanism used by a component; any value >0 is considered to be secure.	Integer	0-9	0	Component
memoryProtection	Determines the level of confidence to memory protection mechanism used by a component; any value >0 is considered to be secure.	Integer	0-9	0	Component
logging	Determines the level of confidence to logging mechanism used by a component; any value >0 is considered to be adequately secure.	Integer	0-9	0	Component
physicalAccessControl	Determines the level of confidence to physical access control mechanism used by a component; any value >0 is considered to be adequate.	Integer	0-9	0	Component
secureBoot	Determines the level of confidence to secure boot mechanism used by a component; any value >0 is considered to be secure.	Integer	0-9	0	Component
sessionAuthenticity	Determines the level of confidence to session authenticity mechanism used by a component; any value >0 is considered to be secure.	Integer	0-9	0	Component
staticCodeAnalysis	Determines the level of confidence to static code analysis performed on a component; any value >0 is considered adequately to be secure.	Integer	0-9	0	Component
strongCryptoAlgorithms	Determines the level of confidence to the cryptographic mechanism used by a component; any value >0 is considered to be secure.	Integer	0-9	0	Component
supplyChainSecurity	Determines the level of confidence to security of supply chain used by a component; any value >0 is considered to be adequately secure.	Integer	0-9	0	Component
systemAccessControl	Determines the level of confidence to access control mechanism used by a component; any value >0 is considered to be adequately secure.	Integer	0-9	0	Component
tamperProtection	Determines the level of confidence to tamper protection mechanism used by a component; any value >0 is considered to be adequately secure.	Integer	0-9	0	Component
userAuthentication	Determines the level of confidence to user authentication mechanism used by a component; any value >0 is considered to be secure.	Integer	0-9	0	Component

Table 2: Threat models used in CRV together with their English and formal descriptions

Name	**English Description / Formal Description**
Location Spoofing	Components which provide the system its geographical positions are unconditionally considered to be susceptible to location spoofing attacks. More precisely, for location spoofing we will instrument components in the given model which are in GPS, IMU, LIDAR, LOCATION_DEVICE categories.
	$\text{CI} = \{\text{C} \mid \text{C.category} = \text{GPS} \lor \text{C.category} = \text{IMU} \lor \text{C.category} = \text{LIDAR} \lor \text{C.category} = \text{LOCATION\_DEVICE}\}$
Insider Threats	Components which are stand-in for human operators with privileges can be susceptible to insider threats unless logging is off, and both system access control and user authentication are disabled.
	$\text{CI} = \{\text{C} \mid \text{C.componentType} \in \{\text{Human, SwHumanHybrid, HwHumanHybrid, Hybrid}\} \land \text{C.insideTrustBoundary} = \text{true} \land (\text{C.logging} = 0 \land (\text{C.systemAccessControl} = 0 \lor \text{C.userAuthentication} = 0))\}$
Outsider Threats	Components which are stand-in for human operators without privileges can be susceptible to outsider threats unless physical access control is enabled and all of the following are also enabled: logging, system access control, and user authentication.
	$\text{CI} = \{\text{C} \mid \text{C.componentType} \in \{\text{Human, SwHumanHybrid, Hybrid, HwHumanHybrid}\} \land \text{C.insideTrustBoundary} = \text{False} \land \text{C.physicalAccessControl} = 0 \land (\text{C.logging} = 0 \land (\text{C.systemAccessControl} = 0 \lor \text{C.userAuthentication} = 0))\}$
Hardware Trojans	Hardware/hybrid components are susceptible to hardware Trojans if they are obtained from commercial off-the-shelf or sourced through a trusted third-party without securing the supply chain and without employing tamper protection.
	$\text{CI} = \{\text{C} \mid \text{C.componentType} \in \{\text{Hardware, SwHwHybrid, HwHumanHybrid, Hybrid}\} \land \text{C.adversariallyTestedForTrojanOrLogicBomb} = 0 \land (\text{C.pedigree} = \text{COTS} \lor (\text{C.pedigree} = \text{Sourced} \land \text{C.supplyChainSecurity} = 0 \land \text{C.tamperProtection} = 0))\}$
Network Injection	Remote network connections that neither employs encryption and authentication are considered to be susceptible to Network Injection attacks.
	$\text{ChI} = \{\text{Ch} \mid (\text{Ch.start.insideTrustedBoundary} = \text{False} \lor \text{Ch.connectionType} = \text{Remote}) \land ((\text{Ch.deviceAuthentication} = 0 \land \text{Ch.sessionAuthenticity} = 0) \lor \text{Ch.start.strongCryptoAlgorithms} = 0)\}$
Remote Code Injection	Software/hybrid components that receive inputs/updates from a remote component without proper security measures are considered to be susceptible to remote code injection attacks.
	$\text{CI} = \{\text{C} \mid \text{C.componentType} \in \{\text{Software, SwHwHybrid, SwHumanHybrid, Hybrid}\} \land (\exists \text{ch} \in \text{C.incomingChannels} : (\text{ch.start.insideTrustBoundary} = \text{False} \lor \text{ch.connectionType} = \text{Remote}) \land \text{ch.start.componentType} \neq \text{Hardware} \land (\text{ch.start.pedigree} = \text{COTS} \lor ((\text{ch.deviceAuthentication} = 0 \land \text{ch.sessionAuthenticity} = 0) \lor \text{ch.start.strongCryptoAlgorithms} = 0))) \land (\text{C.staticCodeAnalysis} = 0 \lor \text{C.inputValidation} = 0 \lor \text{C.memoryProtection} = 0))\}$
Software Malware	Software/hybrid components that receive inputs/updates from a remote component without proper security measures are considered to be susceptible to computer virus/worm/malware attacks.
	$\text{CI} = \{\text{C} \mid \text{C.componentType} \in \{\text{Software, SwHwHybrid, SwHumanHybrid, Hybrid}\} \land (\exists \text{ch} \in \text{C.incomingChannels} : (\text{ch.start.insideTrustBoundary} = \text{False} \lor \text{ch.connectionType} = \text{Remote}) \land \text{ch.start.componentType} \neq \text{Hardware} \land ((\text{ch.start.pedigree} = \text{COTS} \lor (\text{ch.start.pedigree} = \text{Sourced} \land \text{ch.start.supplyChainSecurity} = 0 \land \text{ch.start.tamperProtection} = 0)) \lor ((\text{ch.deviceAuthentication} = 0 \land \text{ch.sessionAuthenticity} = 0) \lor \text{ch.start.strongCryptoAlgorithms} = 0))) \land (\text{C.staticCodeAnalysis} = 0 \lor \text{C.inputValidation} = 0 \lor \text{C.memoryProtection} = 0 \lor \text{C.secureBoot} = 0))\}$
Logic Bomb/Software Trojan	Software/hybrid components that are obtained commercial off-the-shelf or sourced so that they have not been adversarially tested or statically analyzed are susceptible to logic bomb attacks.
	$\text{CI} = \{\text{C} \mid \text{C.componentType} \in \{\text{Software, SwHwHybrid, SwHumanHybrid, Hybrid}\} \land ((\text{C.pedigree} = \text{COTS} \lor (\text{C.pedigree} = \text{Sourced} \land \text{C.supplyChainSecurity} = 0 \land \text{C.tamperProtection} = 0)) \land (\text{C.adversariallyTestedForTrojanOrLogicBomb} = 0 \lor \text{C.staticCodeAnalysis} = 0)\}$