Use case #1: Domestic Medical Device

Exercice 3 – Attack trees

Based on assumption you may define, either list attack path steps, or draw down attack trees related to following threat scenarios

1. “An attacker could pretend to be an authorized phone app to obtain readings from the device”
2. “Invalid input could cause device to crash”

Assuming impact rating as SEVERE for (1) for privacy issues, and MODERATE for (2) for operational issues, compute risk values and propose risk treatment decisions

Use case #1: Domestic Medical Device

Attack paths	Threat types						
	ET	SE	KoIC	WoO	Eq	Value	Feas.
Threat scenario: An attacker could pretend to be an authorized phone app to obtain readings from the device **Attack path:** ➢ Attacker sniffs Bluetooth communications to identify AMPS device ➢ Attacker forge & send an email to patient / victim mimicking clinician team members to retrieve access credentials for system maintenance purposes ➢ Attacker connect to the AMPS device using credentials retrieved from victim, and get access to patient data / PII	1	3	0	4	4	12	High
Threat scenario: Invalid input could cause device to crash **Attack path:** ➢ Attacker sniffs Bluetooth communications to identify AMPS device ➢ Attacker floods / fuzzes AMPS devices using tailored pairing attempts to overload the target	0	6	3	4	4	17	Medium

Ex.3 Attack path analysis

ET elapsed time
SE specialist expertise
KoIC knowledge of the item or component
WoO window of opportunity
Eq equipment

Elapsed time		Specialist expertise		Knowledge of the item or component	
Enumerate	Value	Enumerate	Value	Enumerate	Value
≤1 day	0	Layman	0	Public	0
≤1 week	1	Proficient	3	Restricted	3
≤1 month	4	Expert	6	Confidential	7
≤6 months	17	Multiple experts	8	Strictly confidential	11
>6 months	19				

Window of opportunity		Equipment	
Enumerate	Value	Enumerate	Value
Unlimited	0	Standard	0
Easy	1	Specialized	4
Moderate	4	Bespoke	7
Difficult/ none	10	Multiple bespoke	9

Attack feasibility rating	Values
High	0 - 9
	10 - 13
Medium	14 - 19
Low	20 - 24
Very low	≥ 25

Use case #1: Domestic Medical Device

		Attack feasibility rating			
		Very Low	Low	Medium	High
Impact rating	Severe	2	3	4	5
	Major	1	2	3	4
	Moderate	1	2	2	3
	Negligible	1	1	1	1

Ex.3 Attack path analysis

[13]

Attack paths	Risk metrics		Risk value	Risk treatment decision
	Impact rating	Feasibility rating		
Threat scenario: An attacker could pretend to be an authorized phone app to obtain readings from the device **Attack path:** ➢ Attacker sniffs Bluetooth communications to identify AMPS device ➢ Attacker forge & send an email to patient / victim mimicking clinician team members to retrieve access credentials for system maintenance purposes ➢ Attacker connect to the AMPS device using credentials retrieved from victim, and get access to patient data / PII	Severe	High	5	**Reduce the risk** Access to AMPS device readings / data shall be authenticated using MFA
Threat scenario: Invalid input could cause device to crash **Attack path:** ➢ Attacker sniffs Bluetooth communications to identify AMPS device ➢ Attacker floods / fuzzes AMPS devices using tailored pairing attempts to overload the target	Moderate	Medium	2	**Accept the risk** Rationale: risk of AMPS device crash is communicated to the patient which has to check device status regularly (tbd), and restart if/when crashed