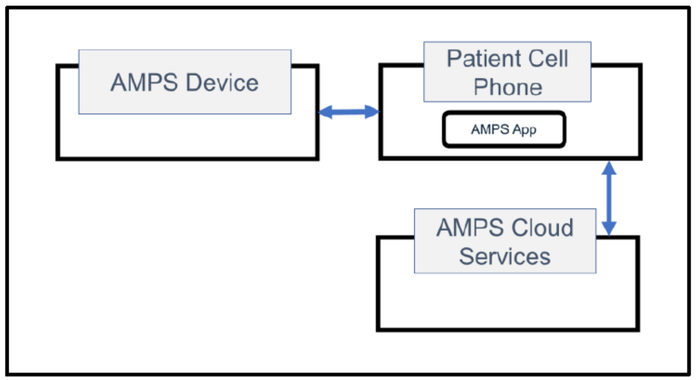
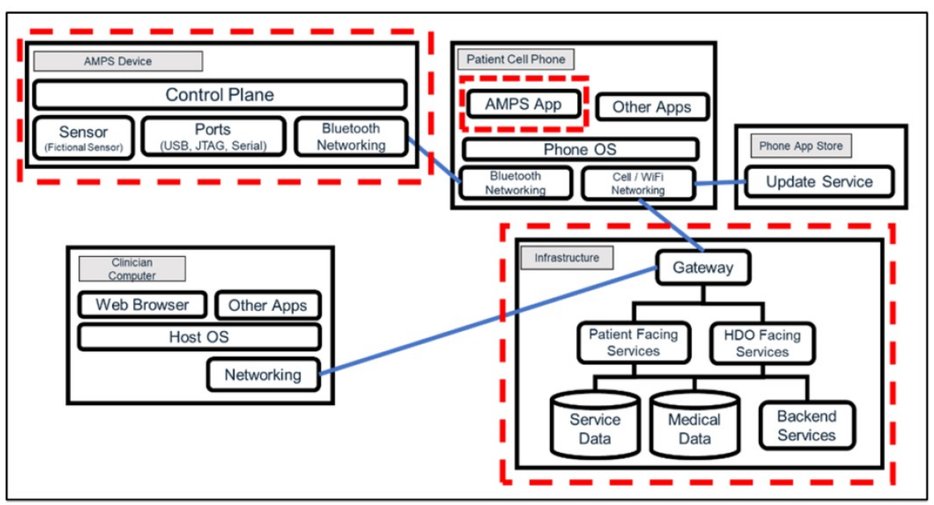
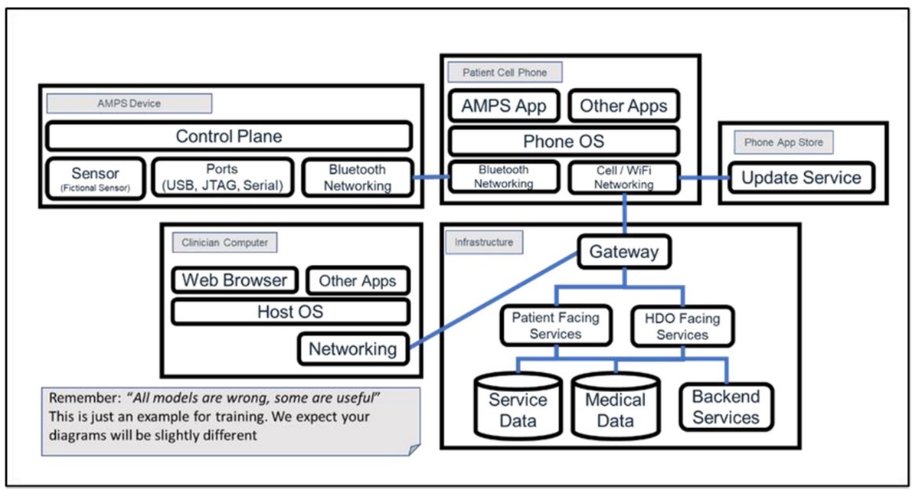
Use case #1: Domestic Medical Device

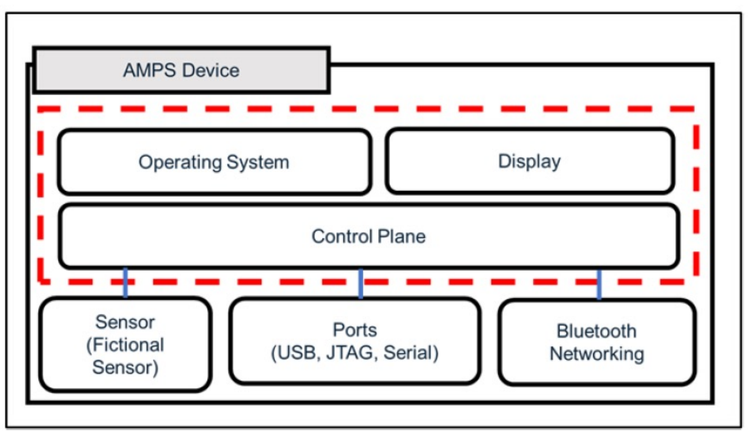




Data Flow Diagram



[13]



swissuniversities

Use case #1: Domestic Medical Device

Threat modelling

Elements	Symbol	Definitions	STRIDE association			
			Ext. Entity	Proc.	Data Store	Data Flow
Spoofing	Tricking a system into believing a falsified entity is a true entity	Using stolen or borrowed credentials to log on as another nurse	X	X		
Tampering	Intentional modification of a system in an unauthorized way	Changing patient data to incorrect values		X	X	X
Repudiation	Disputing the authenticity of an action taken	Denying that a prescribed treatment has been provided to the patient	X	X	?	
Information disclosure	Exposing information intended to have restricted access levels	Health data is sent over an unencrypted Bluetooth connection		X	X	X
Denial of Service (DoS)	Blocking legitimate access or functionality of a system by malicious process(es)	A Bluetooth SpO2 sensor is flooded with bad pairing requests, preventing legitimate connections		X	X	X
Elevation of Privilege (EoP)	Gaining access to functions to which an attacker should not normally have access according to the intended security policy of the product	A patient uses a web portal vulnerability to see all patient data, rather than their own		X		

Use case #1: Domestic Medical Device

Threat modelling

AMPS Component	Spoof	Tamper	Repudiate	Info	DoS	EoP
AMPS Device	1	2			3, 34, 35	4
AMPS App	5, 36	6		7	8	9, 37
App Store	10, 38	11		12	13	14
AMPSCS	15, 39, 40	16,41	17, 42, 43, 44	18, 45	19, 46, 47, 48	20, 49, 50
Clinician Computer	21, 51, 52	22		23	24, 53	25
Dataflow: Bluetooth				26	27, 54	
Dataflow: Cell/Wi-Fi Network		28		29	30	
Dataflow: Clinician Computer Internet		31		32	33	

[13]

Reference ID	STRIDE Type	Description
1	Spoof	An attacker could pretend to be an authorized phone app to obtain readings from the device
2	Tamper	Control plane could be attacked and given incorrect readings
3	DoS	Invalid input could cause device to crash
4	EoP	Device could be hacked, and software could be installed to perform other actions (such as make it part of a botnet, enable lateral movement, etc.)
34	DoS	Software could be corrupted
35	DoS	Battery could be drained more rapidly than normal