CICIoMT2024: A Multi-Protocol Dataset for Assessing IoMT Device Security

Sajjad Dadkhah, Raphael Ferreira, Reginald Chukwuka Molokwu, Euclides Carlos Pinto Neto, Somayeh Sadeghi, Ali A. Ghorbani

The main goal of this research is to propose a realistic benchmark dataset to enable the development and evaluation of IoMT security solutions. To accomplish this, 18 attacks were executed against an IoMT testbed composed of 40 IoMT devices (25 real devices and 15 simulated devices), considering the plurality of protocols used in healthcare (e.g., Wi-Fi, MQTT, and Bluetooth). These attacks are categorized into five classes: DDoS, DoS, Recon, MQTT, and spoofing. This effort aims to establish a baseline complementary to the state-of-the-art contributions and supports researchers in investigating and developing new solutions to make healthcare systems more secure using different mechanisms (e.g., machine learning - ML).

Profiling Experiments

1) Active Experiments: In these captures, the devices were left to interact with one another as people actively (triggering SOS buttons, wearing baby sleep sensor, interacting with apps) or passively (motion detection from cameras) interacted with the devices. MQTT simulated traffic was also included in these captures.

2) Idle Experiments: In these captures, the devices were left alone overnight to observe their idle states.

3) Power Experiments: In these captures, the devices were powered on, and later powered off to observe their power behaviours.

4) Interaction Experiments:
The interaction experiments were carried out by capturing the interaction with devices either physically or through their companion apps. Wherever applicable, each possible interaction was done either on the LAN or WAN:

Cameras (Blink/Ecobee/M1T/Owltron):
----

i) LAN_MIC: In these experiments, the mic of the camera was turned on through their respective companion apps for the duration of the capture. The companion app was connected to the same network as the camera.

ii) LAN_WATCH: In these experiments, the companion app was used to watch the live feed of the camera. The companion app was connected to the same network as the device.

iii) LAN_PHOTO: In these experiments, the companion app was used to capture a photo of the camera's live feed. The companion app was connected to the same network as the device.

iv) LAN_RECORDING: In these experiments, the companion app was used to record the camera's live feed. The companion app was connected to the same network as the device.

v) WAN_MIC: In these experiments, the mic of the camera was turned on through their respective companion apps for the duration of the capture. The companion app was connected to a different network as the camera.

vi) WAN_WATCH: In these experiments, the companion app was used to watch the live feed of the camera. The companion app was connected to a different network as the device.

vii) WAN_PHOTO: In these experiments, the companion app was used to capture a photo of the camera's live feed. The companion app was connected to a different network as the device.

viii) WAN_RECORDING: In these experiments, the companion app was used to record the camera's live feed. The companion app was connected to a different network as the device.

Multifunctional Pager:
----
i) LAN_APP: In these experiments, the companion app was used to interact with the device, and change their security profiles (Home, Armed, Away). The companion app was connected to the same network as the device.

ii) LAN_PHYSICAL: In these experiments, the pager button was physically pressed to trigger an emergency alarm on the companion app, and the respective base station. The companion app was connected to the same network as the device.

iii) WAN_APP : In these experiments, the companion app was used to interact with the device, and change their security profiles (Home, Armed, Away). The companion app was connected to a different network as the device.

iv) WAN_PHYSICAL: In these experiments, the pager button was physically pressed to trigger an emergency alarm on the companion app, and the respective base station. The companion app was connected to a different network as the device.

SenseU:
----
i) LAN_EMERGENCY: In these experiments, the sensor was physically oriented to trigger an emergency alarm on the companion app, and the respective base station. The companion app was connected to the same network as the device.

ii) WAN_EMERGENCY: In these experiments, the sensor was physically oriented to trigger an emergency alarm on the companion app, and the respective base station. The companion app was connected to a different network as the device.

Singcall:
----
i) LAN_PHYSICAL: In these experiments, the pager button was physically pressed to trigger an emergency on the companion app. The companion app was connected to the same network as the device.

ii) WAN_PHYSICAL: In these experiments, the pager button was physially pressed to trigger an emergency on the companion app. The companion app was connected to a different network as the device.