

Cyber-Security for BLE Medical Devices

July 2021

H3 System, Co., Ltd.

Min-Joon Kim

1 Cyber-Security Guidelines in Korea



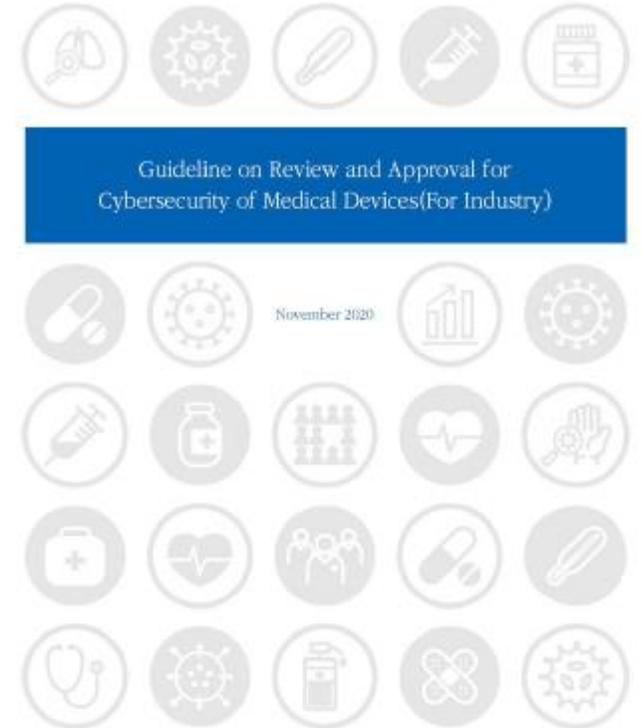
의료기기의 사이버 보안 허가 · 심사
가이드라인 (민원인 안내서)

2019. 11. 28



의료기기의 사이버 보안 적용방법
및 사례집(민원인 안내서)

2019. 11. 28



2

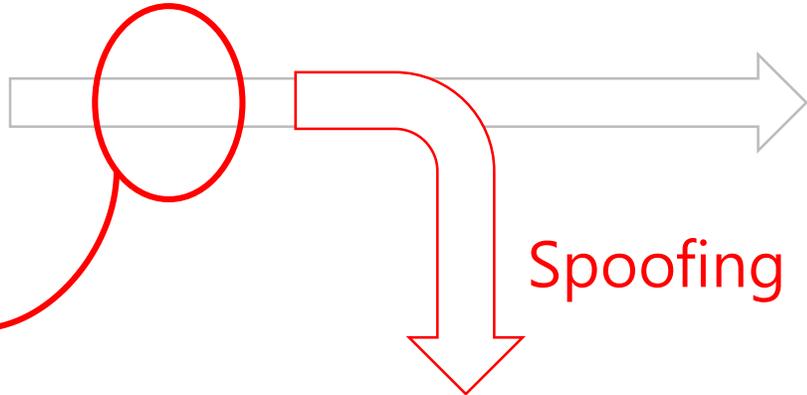
Cyber-Security and COVID-19



The image shows a screenshot of a HIMSS website article. The header includes the HIMSS logo and navigation links: WHO WE ARE, WHAT WE DO, MEMBERSHIP, RESOURCES, NEWS, and EVENTS. Below the header, the text 'QUALITY CARE' is displayed. The main title of the article is 'Remote Patient Monitoring: COVID-19 Applications and Policy Challenges' in a large, bold, italicized font. Below the title, it says 'Published on March 31, 2020'. At the bottom of the screenshot, there is a photograph of a person's hands holding a smartphone. The phone screen displays a health monitoring application with a heart rate of 118, a temperature of 75, and a blood pressure of 85.

3

Probable attacks on BLE communications



Sniffing

Spoofing



4

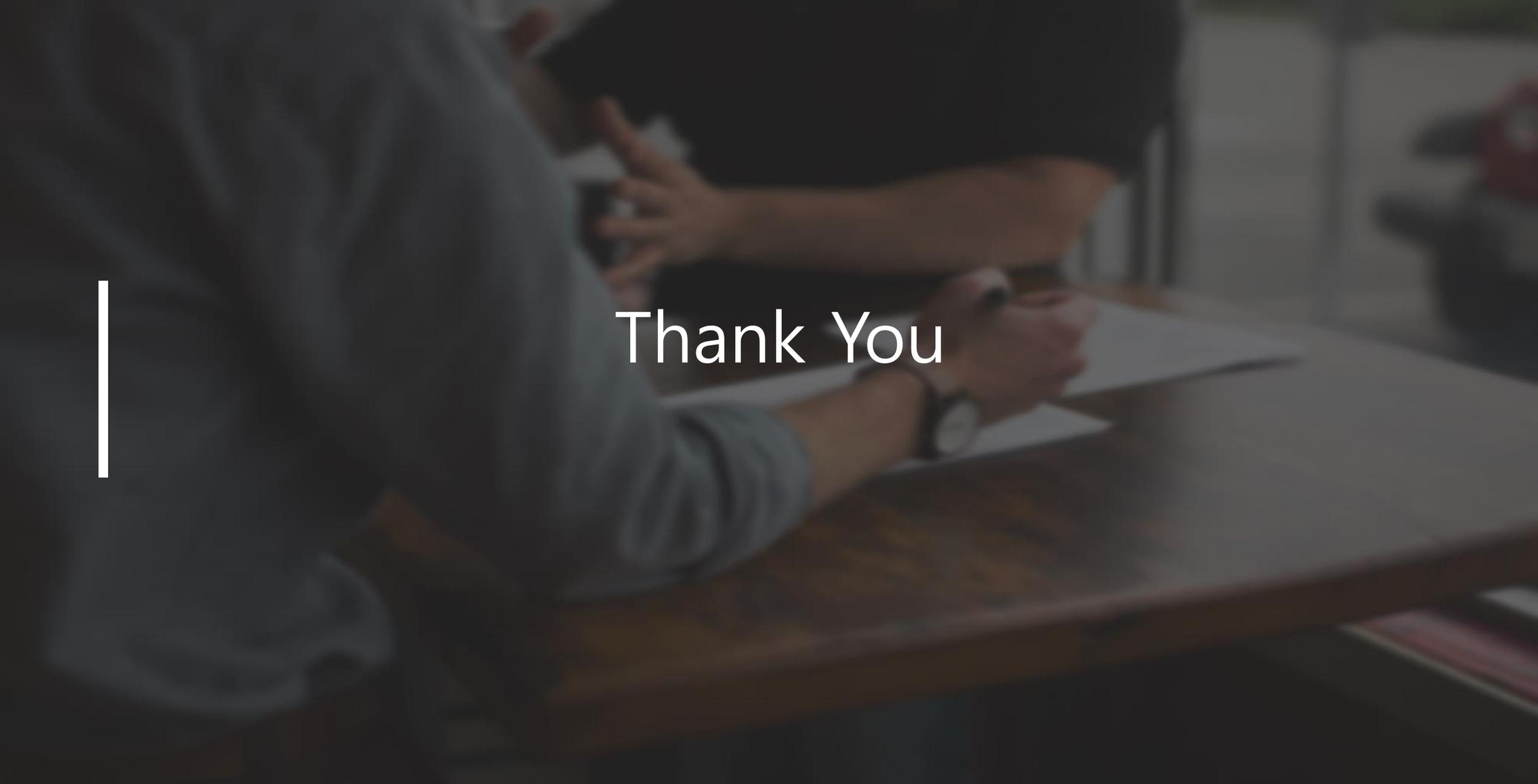
BLE Communication Perspectives

- Recommended BLE Security level for high-risk devices
 - BLE 4.0/4.1: Security level 3
 - BLE 4.2 or later: Security level 4
- Pairing/Bonding
 - MITM(Man In The Middle)
 - Numeric comparison, Passkey Entry, or OOB(Out of Band)
- LESEC(LE Secure Connection)

5

UX Perspectives

- Separate pairing process and data transfer process
 - For data transfer, minimize users' intervention to increase usability.
 - For pairing, special users' action(for example, press and hold a button for a long time) is required although it's not easy for some users.
 - The whitelist feature in Bluetooth connection is generally followed.



Thank You