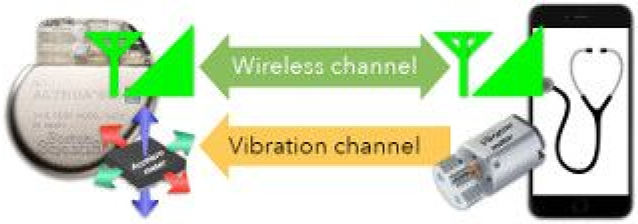
Dr. Kim Speaks to Our Section about Medical IoT Security

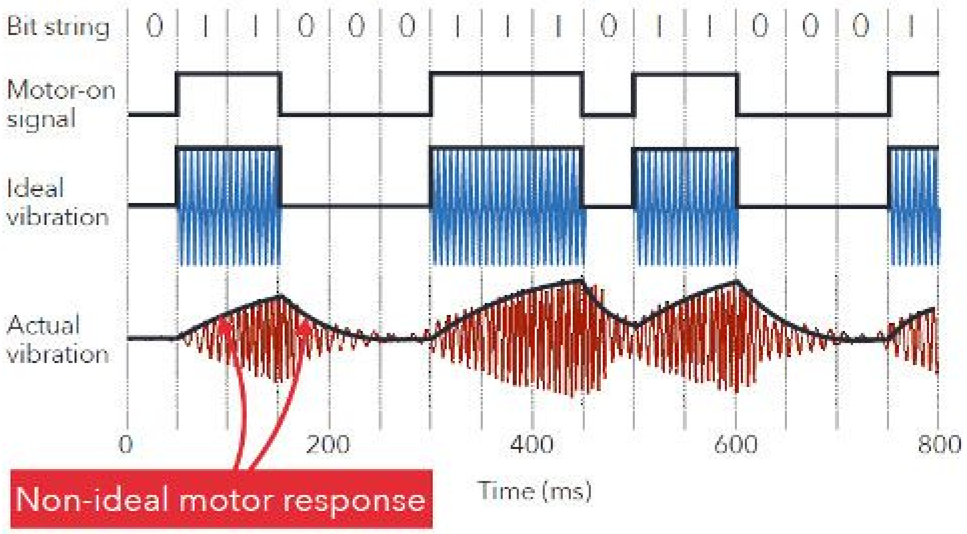
At our January meeting, Dr. Younghyun Kim spoke about an technique for privately sharing an encryption key for medical devices.

Kim told us about an episode of *Homeland* in which a hacker sabotages a pacemaker. This is not far-fetched. There are some medical products with controls that can be actuated wirelessly with no encryption. Former Vice President Dick Cheney had the wireless functionality of his pacemaker disabled due to these concerns.

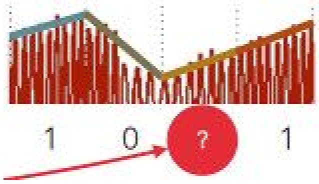
One reason for not encrypting is to save power. Medical devices sometimes have no charging capability and require a medical procedure to replace that battery. A public shared key encryption scheme would require too much power. An alternative is to share the key using the vibrations of a haptic motor.



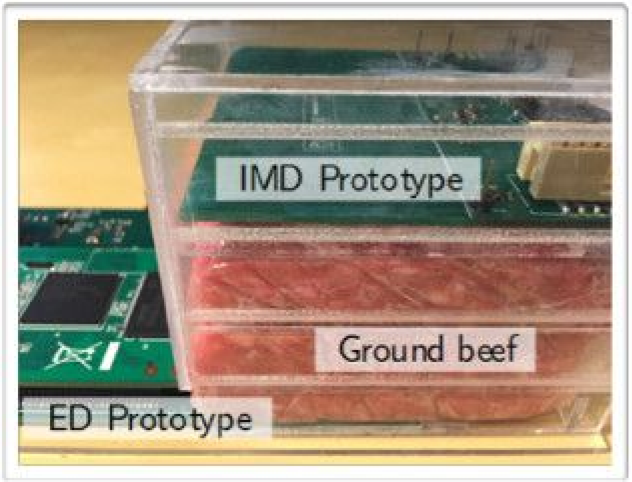
The password can be encoded using basic on-off-keying (OOK). The receiver side has to look at not just the the amplitude but also the slope because it takes some time for the motor to spin up or slow down.   A typical haptic motor vibrates at in the 100 to 200 Hz range. This is the "carrier" on which the OOK message is modulated. Data rates in the 20 bps range are possible. Vibrations from human motion are other frequencies, so a bandpass filter can isolate the carrier and filter out extraneous vibrations, similar to a radio receiver.



If a bit cannot be recovered due to intersymbol interference, the receiver can simply try all the possible bits until it finds the one that works. It could also request over the RF link that particular bits be resent.



The test setup to simulate a receiver inside the body detecting vibrations from a transmitter outside the body.



As an added protection, the speaker can produce noise with spectral components in the 100-200Hz range to prevent a microphone from decoding the message from a distance.

The advantages of this scheme are:

1. Short range - So the key need not be a publically shared key, which would require more processing power.
2. Small power consumption
3. High perceptibility - If a hacker sends vibrations to the medical device, the user can feel it.
4. Most mobile devices have haptic vibration motors.