Younghyun Kim

Assistant Professor

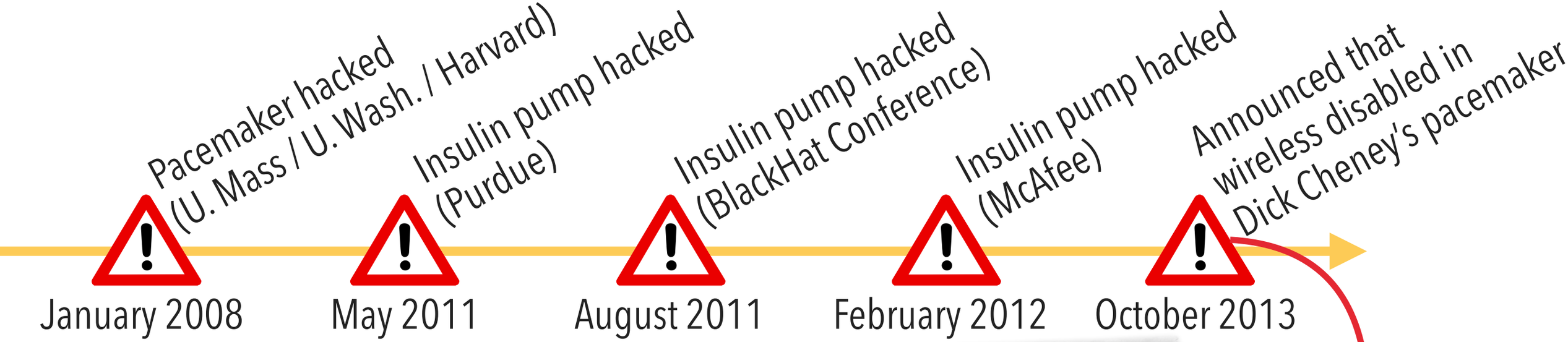
Department of Electrical and Computer Engineering

University of Wisconsin–Madison

Challenges and Solutions in IoT End-Point Security: A Case for Implantable Medical IoT

U.S.-Korea Forum on Nanotechnology, Sep. 12, 2017

"Disconnected to Save ~~Battery~~ My Life"



The Washington Post

"... former Vice President Dick Cheney revealed that his doctor ordered the wireless functionality of his heart implant ***disabled due to fears it might be hacked in an assassination attempt****."*

October 21, 2013.

Challenges in IWMDs Security

Security

Limited energy

Power-hungry security techniques (e.g., public key encryption) are not feasible

Limited user interface

Traditional user-operated security techniques (e.g., PIN, fingerprint) are not feasible

Unique usage model (Security vs. Safety)

Prompt access should be granted in an emergency when patient is unconscious

Solutions for Secure and Energy-Efficient Connectivity

SecureVibe

Vibration-based side channel for secure wireless connection establishment

TeleProbe

LC-tank based inductive coupling for zero-power communication

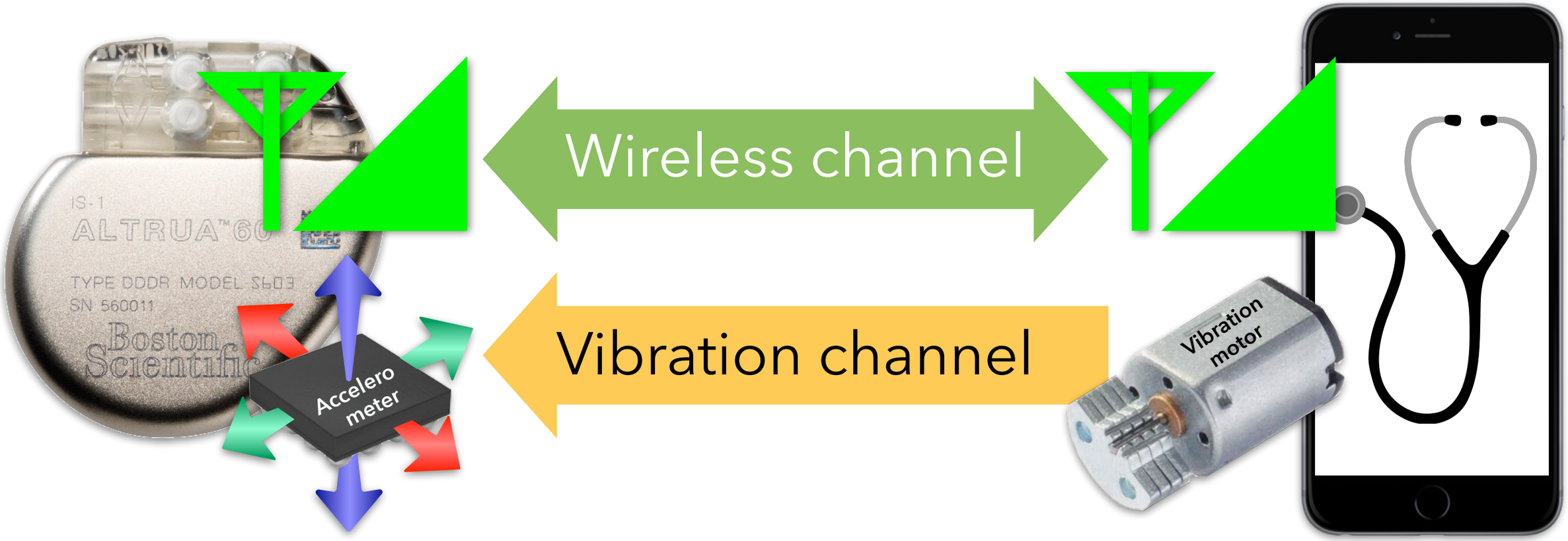
Key Idea: Vibration-based Side Channel

Short transmission range (direct contact required)

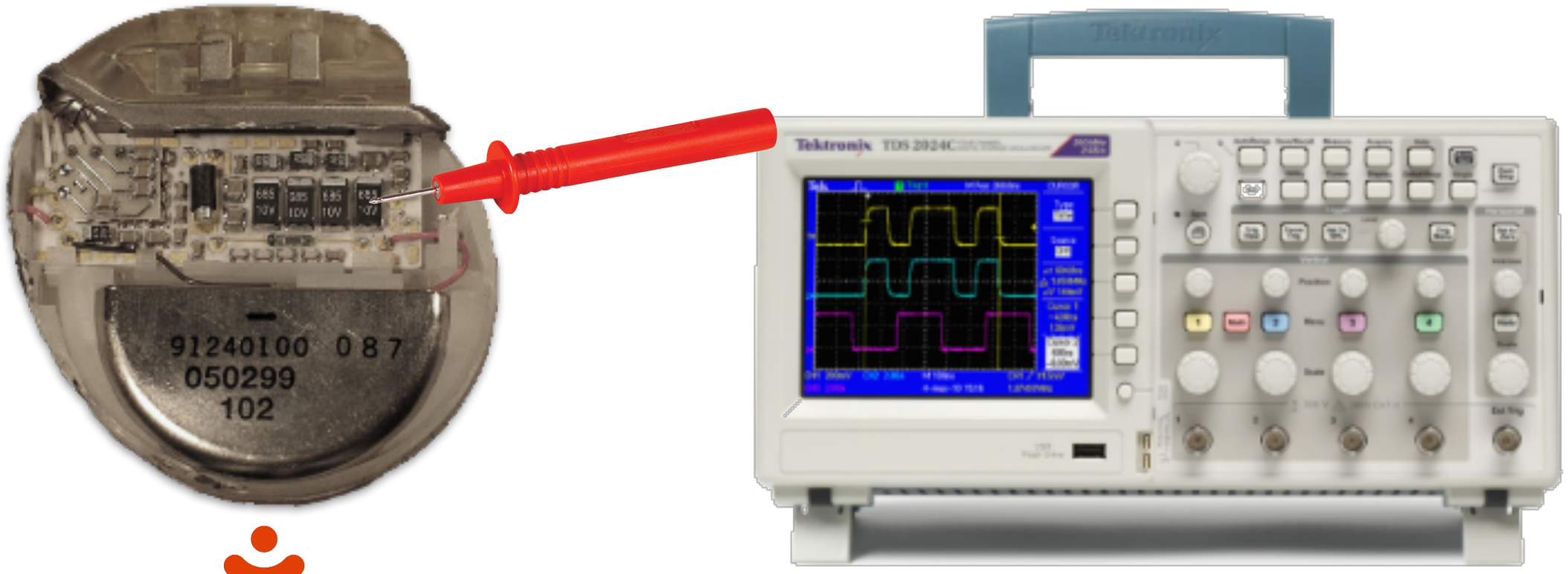
High perceptibility

Low power consumption and small footprint

Ubiquitous transmitters (e.g., smartphones)



Wireless Probing of Implantable Medical Devices



Continuous signal posing
in implantation
(e.g., ECG, EMG, blood glucose)

Challenges in ~~IWMDs~~ IoT Security

Security

Limited energy

IoT end-point devices are untethered, relying on limited batteries or energy harvesting

Low-power security

Limited user interface

IoT end-point devices are deeply embedded and have a stringent form-factor constraint

Small-footprint HCI

Unique usage model

IoT end-point devices have unique usage models

Application- and domain-specific security