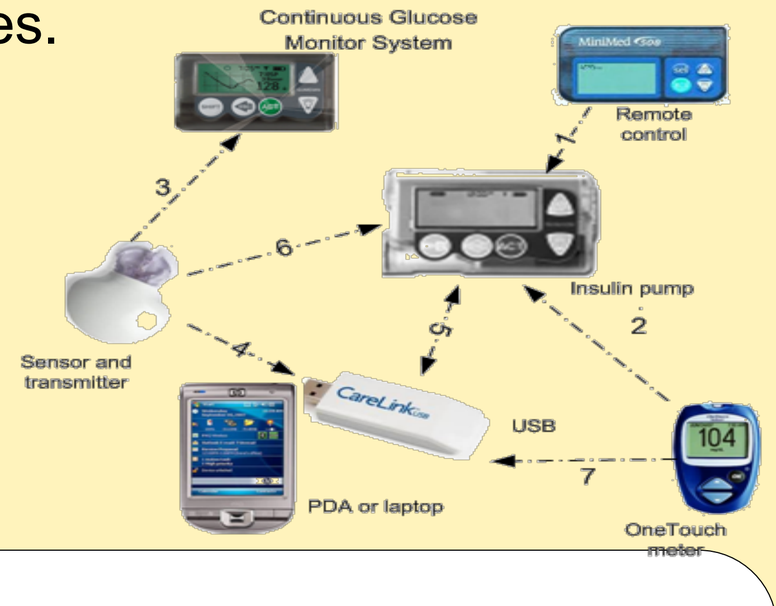
CPS security for insulin pumps

Dr. Xiali (Sharon) Hei, Delaware State University
www.xialihei.com


Lead PI Phot

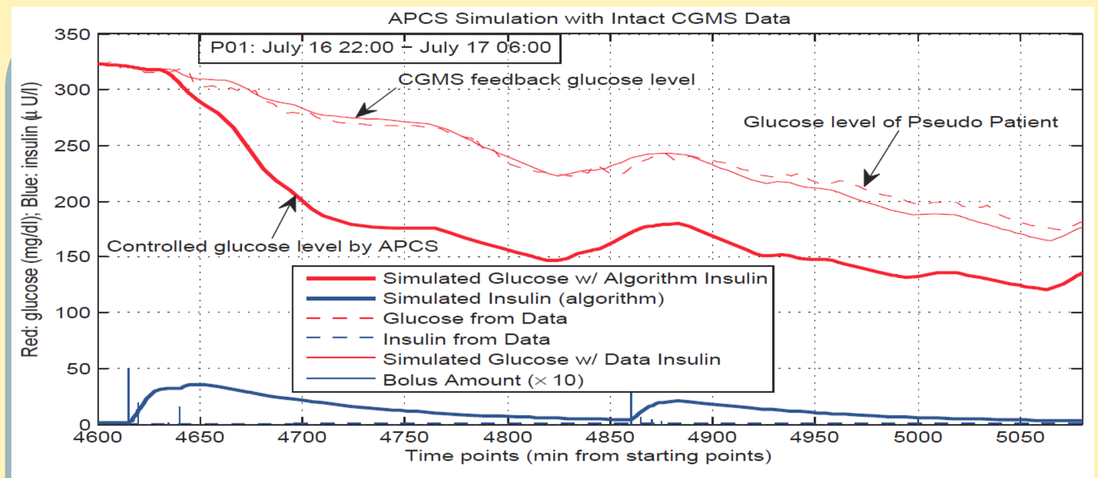
Motivation

The objective of this project is to protect the two important wireless links in the insulin pump system. We are trying to build an abnormal model to detect the glucose level attacks of glucose sensors. Also, we are building acoustic and other side channels for implantable medical devices.

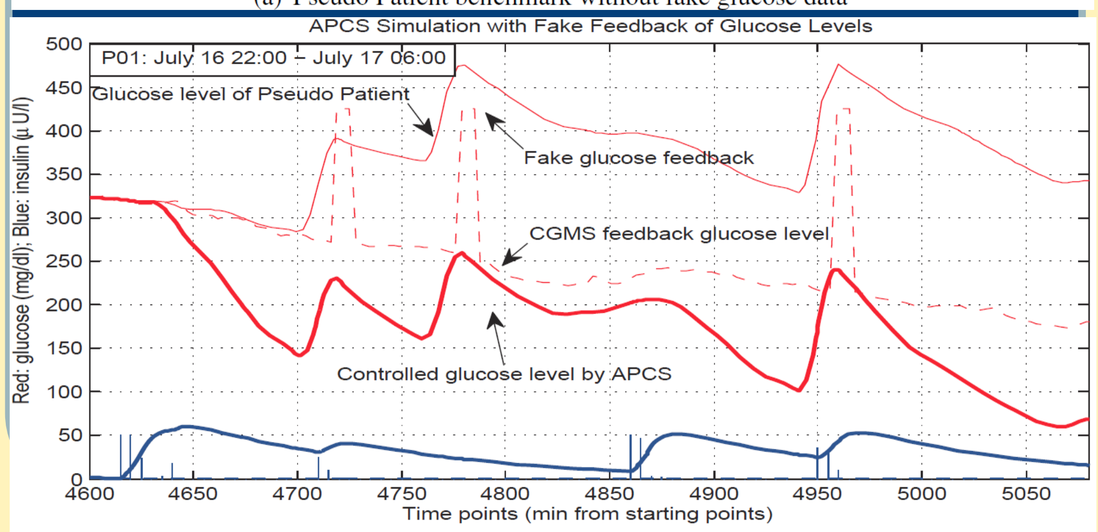


In 2014, 29.1 million people in the USA were diagnosed with diabetes. Nowadays, about 550,000 patients used an insulin pump.

These wireless medical devices need to be reliable, secure, and safe.



(a) Pseudo Patient benchmark without fake glucose data



(b) Glucose level attack 1

Approach

Abnormal glucose level attack detection

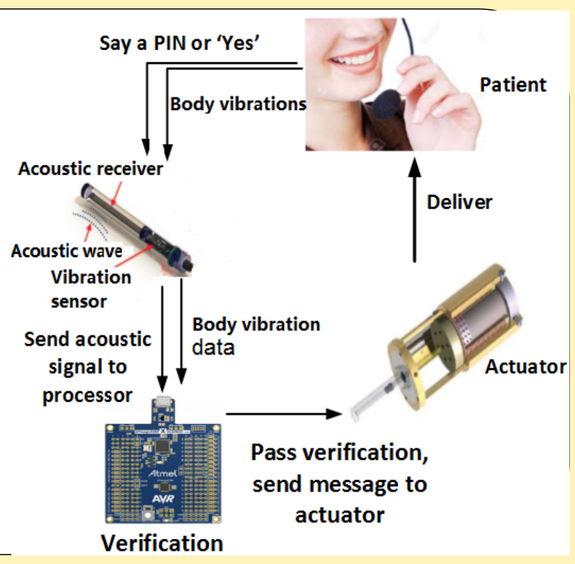
- A mathematical model to calculate the expected glucose level based on patient physiological parameters
- Model optimization

Out of band secure channels

- Acoustic channels (device fingerprinting)
- Magnetic channels

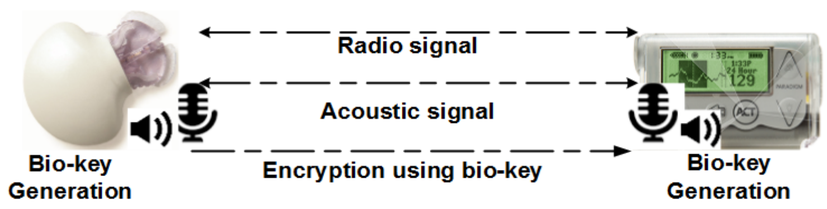
Acoustic channel:

Voice print authentication



Acoustic channel (cont.)

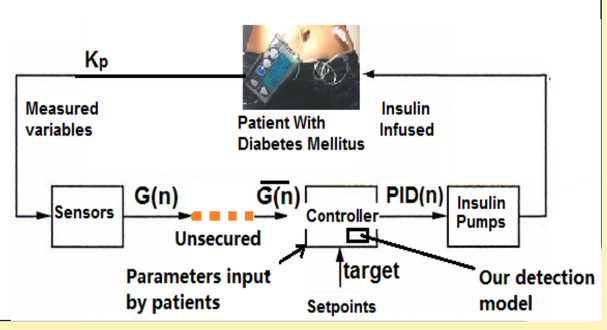
Device fingerprinting



New CPS attacks

Possible forged glucose levels to attack the PID controller

$$\overline{G(n)} = target \times (1+\varepsilon)$$
$$\overline{G(n)} = target + A(-1)^n$$



Glucose abnormal detection model

$$PID(n) = \delta(G(n), G(n-1), PID(n-1), target, parameters)$$
$$\overline{G(n)} = \delta(\overline{G(n)}, PID(n), U_C(n), G(n-1), PID(n-1), target, parameters)$$

If $|G(n) - \overline{G(n)}| > \varepsilon$, there is an attack

Interested in meeting the PIs? Attach post-it note below!
Or email me: xhei@desu.edu

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Jan 9-11th, 2017
Arlington, VA

DSU Delaware State University