GlucOS: Security, correctness, and simplicity for automated insulin delivery

Hari Venugopalan, Shreyas Madhav Ambattur Vijayanand, Caleb Stanford, Stephanie Crossen and Samuel T. King

UCDAVIS
UNIVERSITY OF CALIFORNIA

Biohacker

/ˈbīōˌhakər/

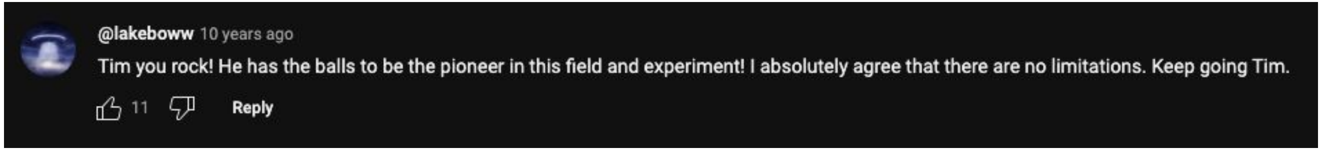
Noun

1. A person who manipulates their metabolic state using sensors, injected hormones, nutrients, physical activity, computer systems, and AI
2. An enthusiastic and curious person who learns about their own biology and metabolism through experimentation on themself
3. A person who uses computers to gain access to someone’s metabolic state

Biohackers

https://bioengineer.org/biohacker-implants-chip-arm/

Biohackers

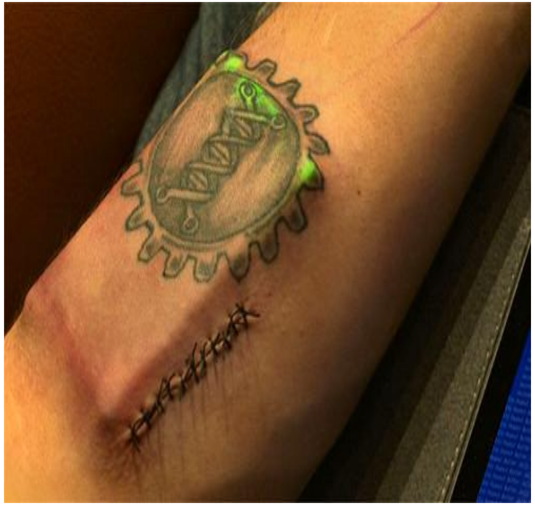


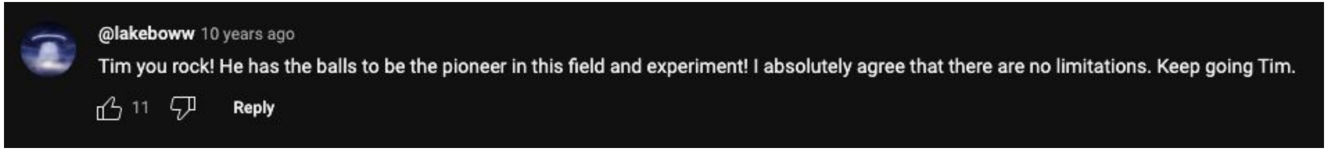
@lakeboww 10 years ago

Tim you rock! He has the balls to be the pioneer in this field and experiment! I absolutely agree that there are no limitations. Keep going Tim.

https://bioengineer.org/biohacker-implants-chip-arm/
https://www.youtube.com/watch?v=clIiP1H3Opw

Biohackers

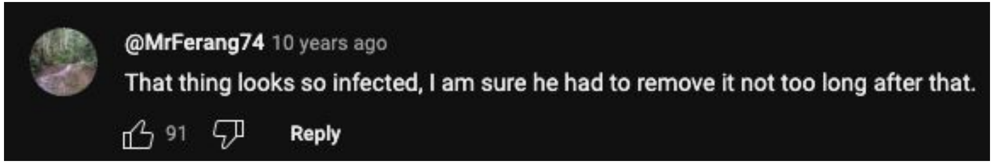




@lakeboww 10 years ago

Tim you rock! He has the balls to be the pioneer in this field and experiment! I absolutely agree that there are no limitations. Keep going Tim.

👍 11 👎 Reply



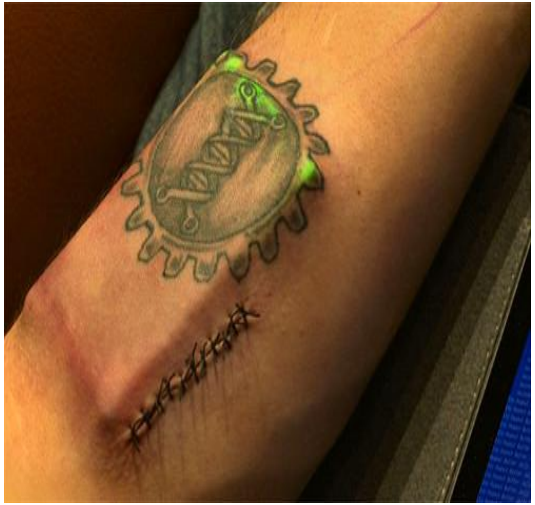
@MrFerang74 10 years ago

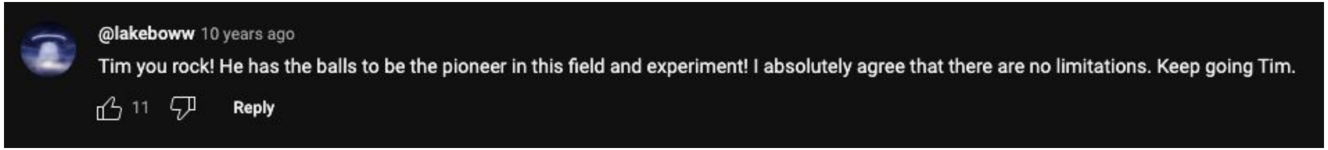
That thing looks so infected, I am sure he had to remove it not too long after that.

👍 91 👎 Reply

https://bioengineer.org/biohacker-implants-chip-arm/
https://www.youtube.com/watch?v=clIiP1H3Opw

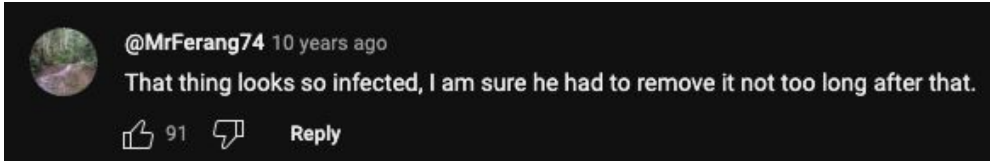
Biohackers





@lakeboww 10 years ago

Tim you rock! He has the balls to be the pioneer in this field and experiment! I absolutely agree that there are no limitations. Keep going Tim.



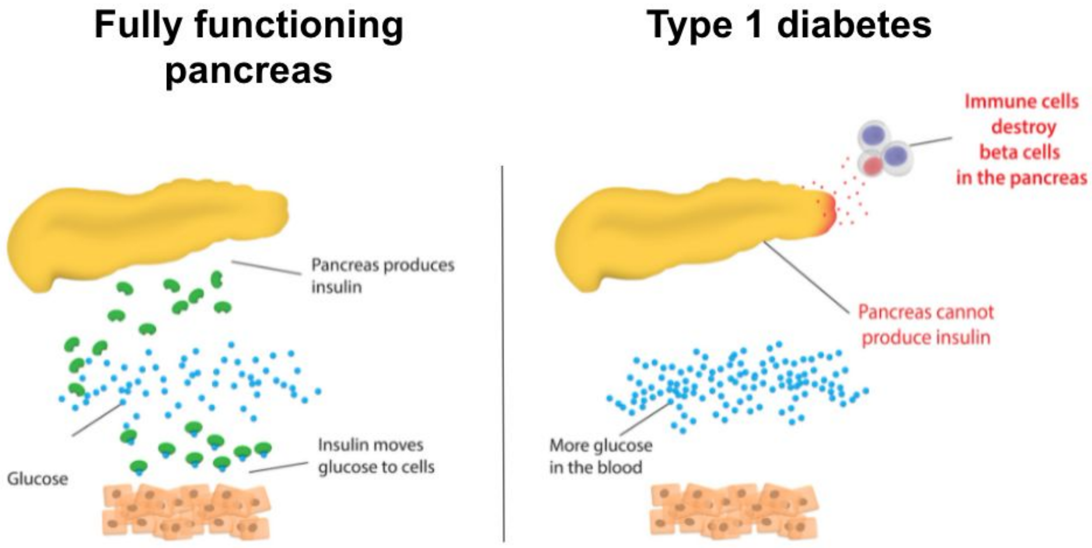
@MrFerang74 10 years ago

That thing looks so infected, I am sure he had to remove it not too long after that.

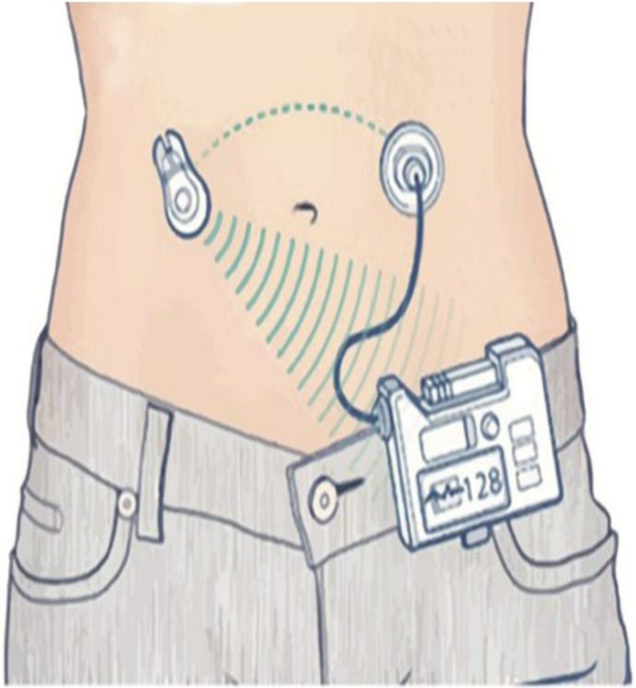
8.4 million people live with type 1 diabetes and they’re the most hardcore Biohackers

https://bioengineer.org/biohacker-implants-chip-arm/
https://www.youtube.com/watch?v=clIiP1H3Opw

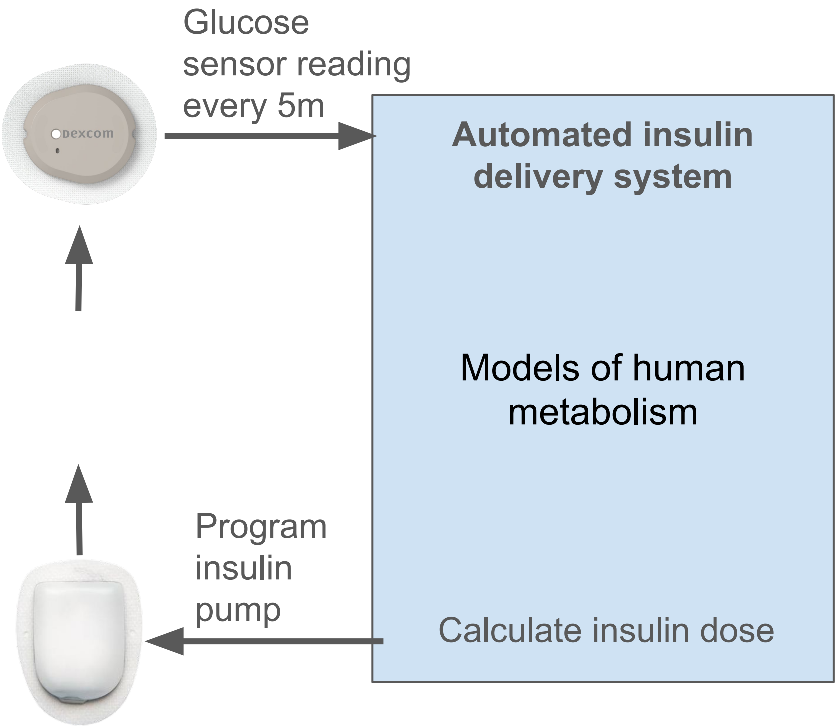
Overview of type 1 diabetes


Fully functioning pancreas
Pancreas produces insulin
Glucose
Insulin moves glucose to cells
Type 1 diabetes
Immune cells destroy beta cells in the pancreas
Pancreas cannot produce insulin
More glucose in the blood

Automated insulin delivery systems



https://www.breakthrought1d.org/



Glucose sensor reading every 5m

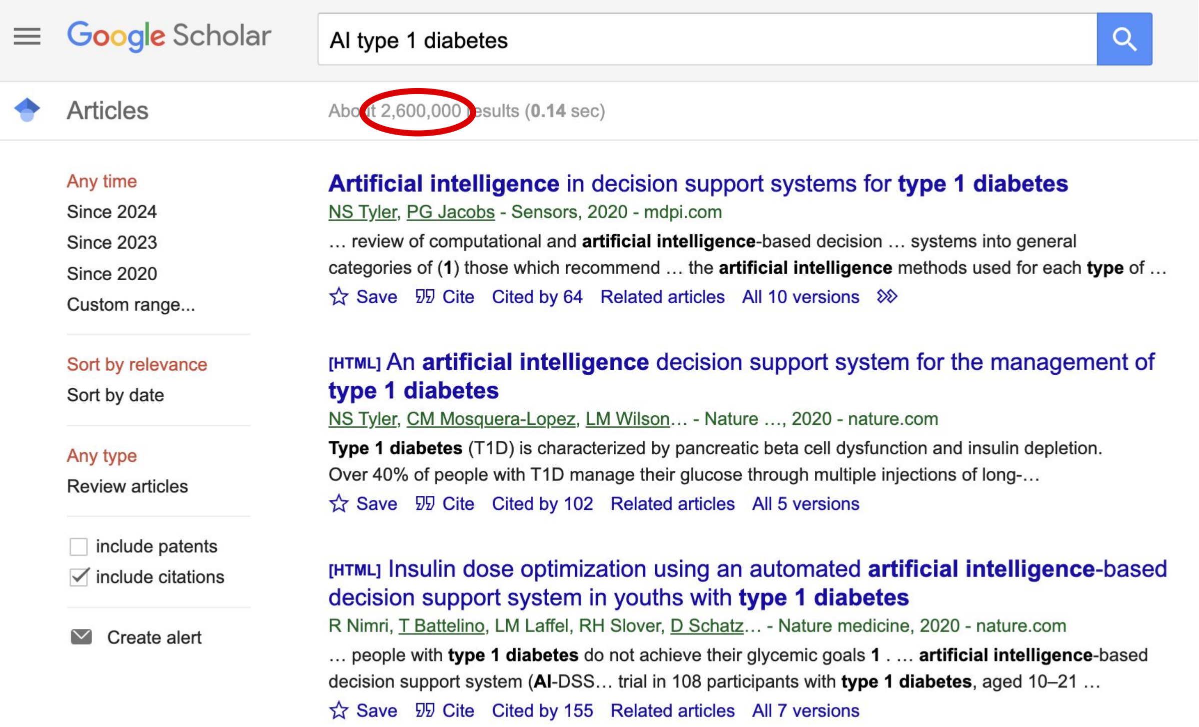
Automated insulin delivery system

Models of human metabolism

Calculate insulin dose

Program insulin pump

ML to calculate insulin doses?



Google Scholar

AI type 1 diabetes

Articles

About 2,600,000 results (**0.14** sec)

Any time

Since 2024

Since 2023

Since 2020

Custom range...

Sort by relevance

Sort by date

Any type

Review articles

□ include patents

☑ include citations

Create alert

Artificial intelligence in decision support systems for **type 1 diabetes**

NS Tyler, PG Jacobs - Sensors, 2020 - mdpi.com

… review of computational and **artificial intelligence**-based decision … systems into general categories of (**1**) those which recommend … the **artificial intelligence** methods used for each **type** of …

☆ Save 99 Cite Cited by 64 Related articles All 10 versions

[HTML] An **artificial intelligence** decision support system for the management of **type 1 diabetes**

NS Tyler, CM Mosquera-Lopez, LM Wilson… - Nature …, 2020 - nature.com

Type 1 diabetes (T1D) is characterized by pancreatic beta cell dysfunction and insulin depletion. Over 40% of people with T1D manage their glucose through multiple injections of long-…

☆ Save 99 Cite Cited by 102 Related articles All 5 versions

[HTML] Insulin dose optimization using an automated **artificial intelligence**-based decision support system in youths with **type 1 diabetes**

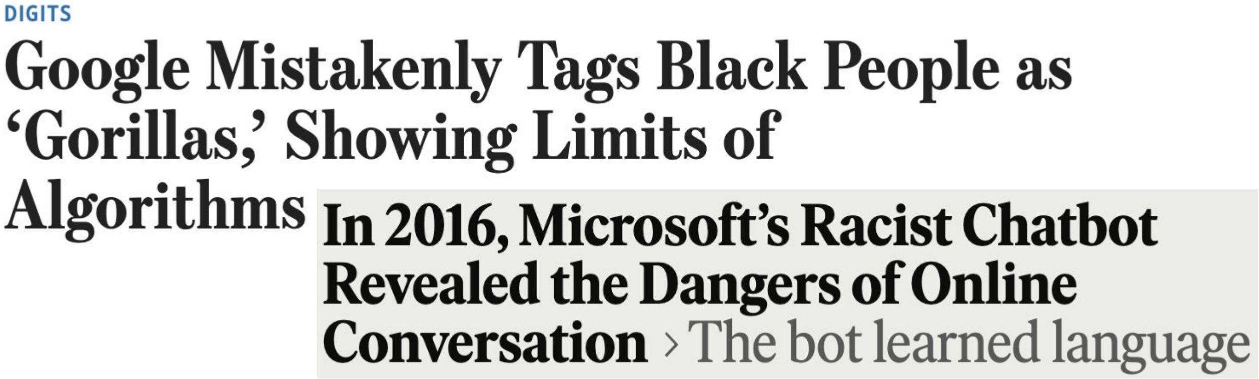
R Nimri, T Battelino, LM Laffel, RH Slover, D Schatz… - Nature medicine, 2020 - nature.com

… people with **type 1 diabetes** do not achieve their glycemic goals **1** . … **artificial intelligence**-based decision support system (**AI**-DSS… trial in 108 participants with **type 1 diabetes**, aged 10–21 …

☆ Save 99 Cite Cited by 155 Related articles All 7 versions

Current automated insulin delivery systems do NOT use the most advanced ML, like deep neural networks!

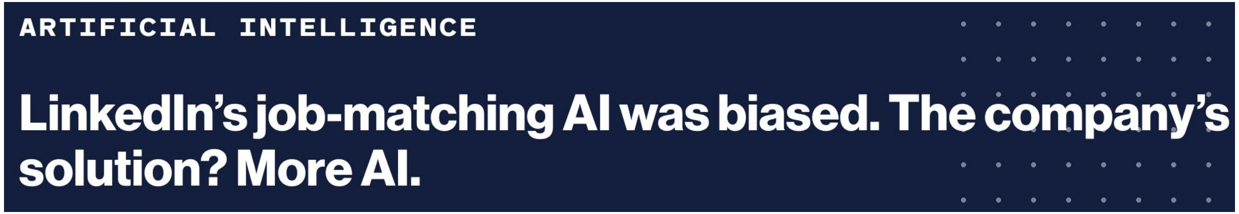
ML will always make mistakes in ways that are difficult to anticipate



DIGITS

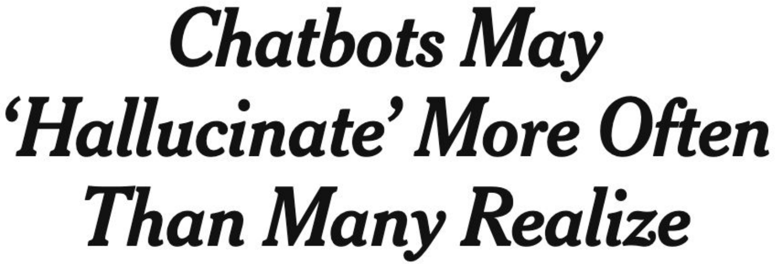
Google Mistakenly Tags Black People as 'Gorillas,' Showing Limits of Algorithms

In 2016, Microsoft's Racist Chatbot Revealed the Dangers of Online Conversation › The bot learned language



ARTIFICIAL INTELLIGENCE

LinkedIn's job-matching AI was biased. The company's solution? More AI.



Chatbots May 'Hallucinate' More Often Than Many Realize

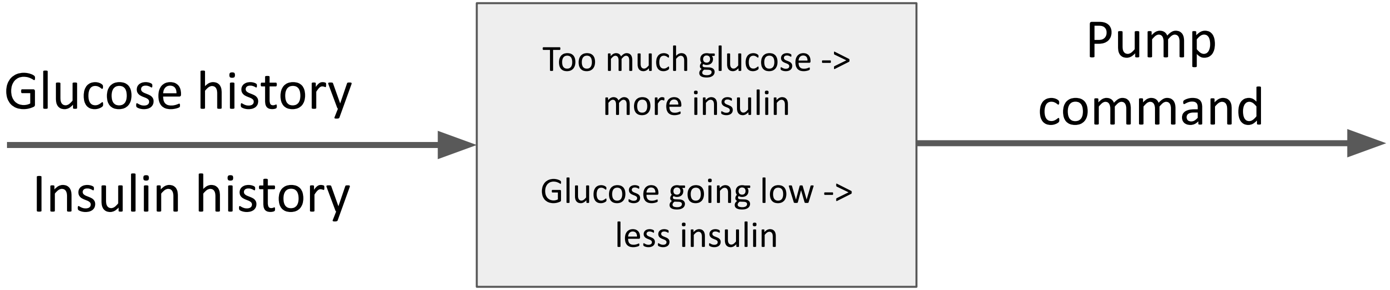
GlucOS: End-to-end system for trustworthy insulin delivery

- Algorithmic security
- Driver security
- End-to-end security incorporating formal methods
- Keeping humans in the loop

Design, implement, and deploy a system on real humans to help manage their Type 1 Diabetes

Algorithmic Security

Reactive models



Glucose history

Insulin history

Too much glucose -> more insulin

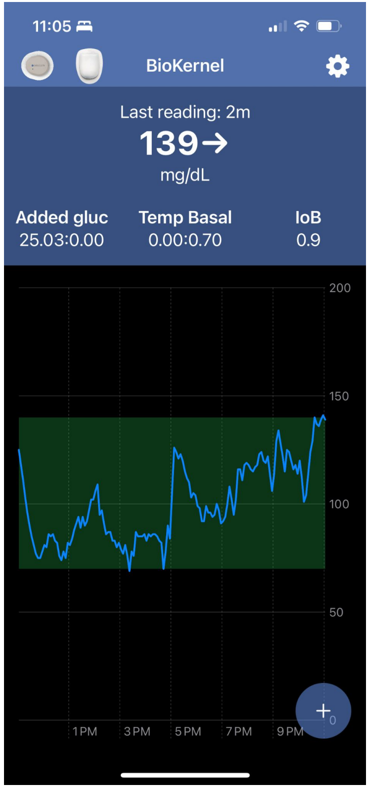
Glucose going low -> less insulin

Pump command

- Pros: Simple and safe
- Cons: Slow and thus poor control

ML for automatic and predictive insulin dosing

Scenario from a real user who ate a snack at around 9pm but doesn't have enough insulin on board for full digestion



11:05

BioKernel

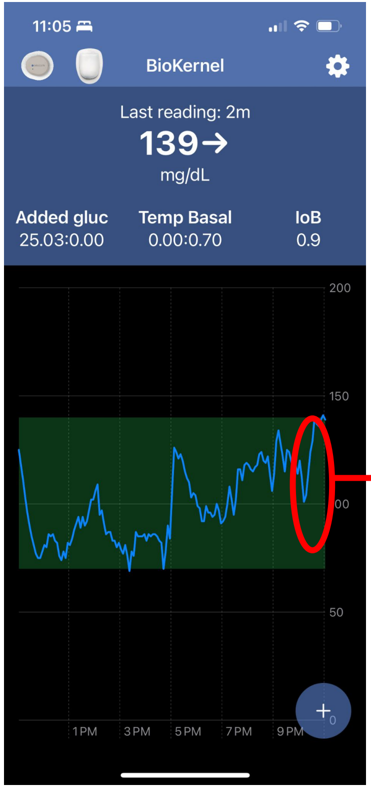
Last reading: 2m

139→

mg/dL

Added gluc	Temp Basal	IoB
25.03:0.00	0.00:0.70	0.9

ML for automatic and predictive insulin dosing



11:05

BioKernel

Last reading: 2m

139→

mg/dL

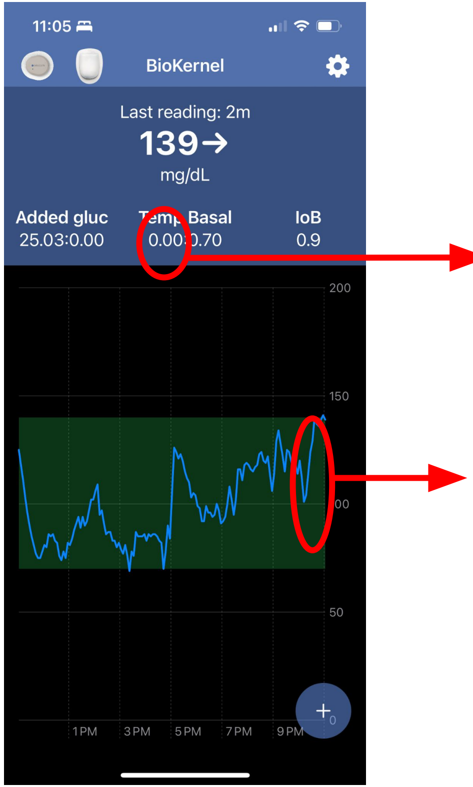
Added gluc 25.03:0.00

Temp Basal 0.00:0.70

IoB 0.9

Digestion starting, glucose in range

ML for automatic and predictive insulin dosing



11:05

BioKernel

Last reading: 2m

139→

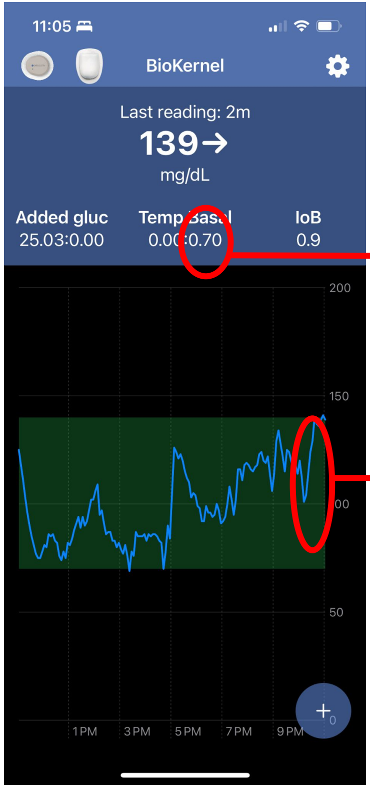
mg/dL

Added gluc	Temp Basal	IoB
25.03:0.00	0.00:0.70	0.9

The reactive safe model thinks there is sufficient insulin on board

Digestion starting, glucose in range

ML for automatic and predictive insulin dosing



11:05

BioKernel

Last reading: 2m

139→

mg/dL

Added gluc 25.03:0.00

Temp Basal 0.00:0.70

IoB 0.9

Predictive ML starts injecting more insulin

Digestion starting, glucose in range

Insight for ML security

All correct insulin dosing algorithms will dose the same amount over a long enough time

Insight for ML security

All correct insulin dosing algorithms will dose the same amount over a long enough time

But the timing of when you inject matters A LOT

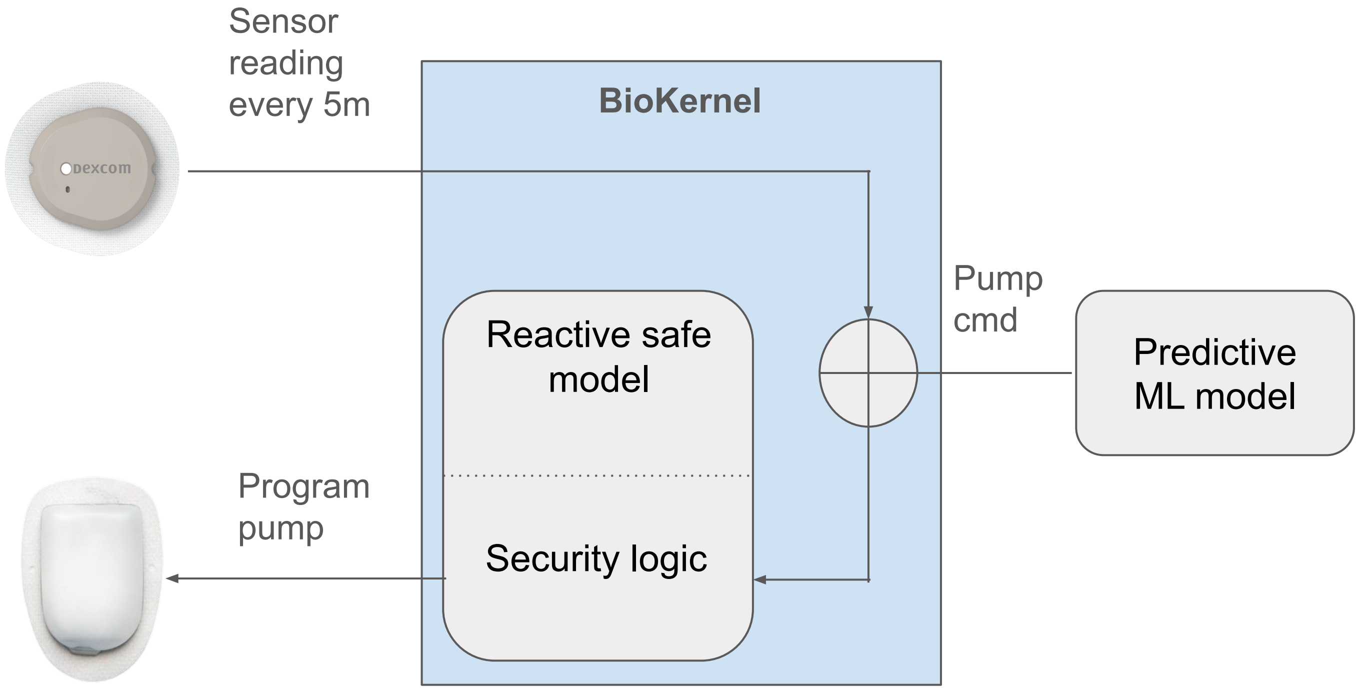
Insight for ML security

All correct insulin dosing algorithms will dose the same amount over a long enough time

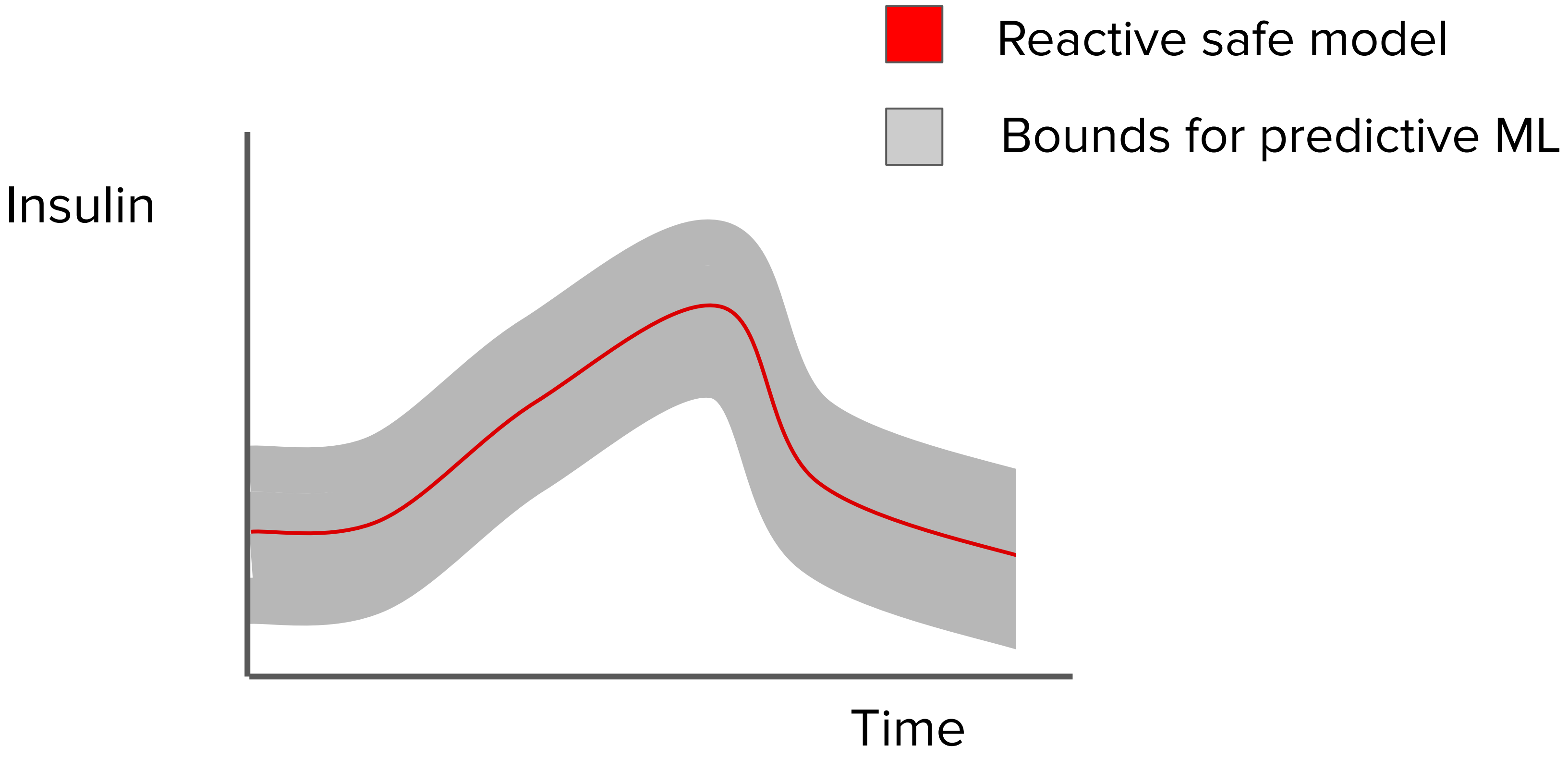
But the timing of when you inject matters A LOT

Rather than getting rid of the reactive safe model, we repurpose it for security

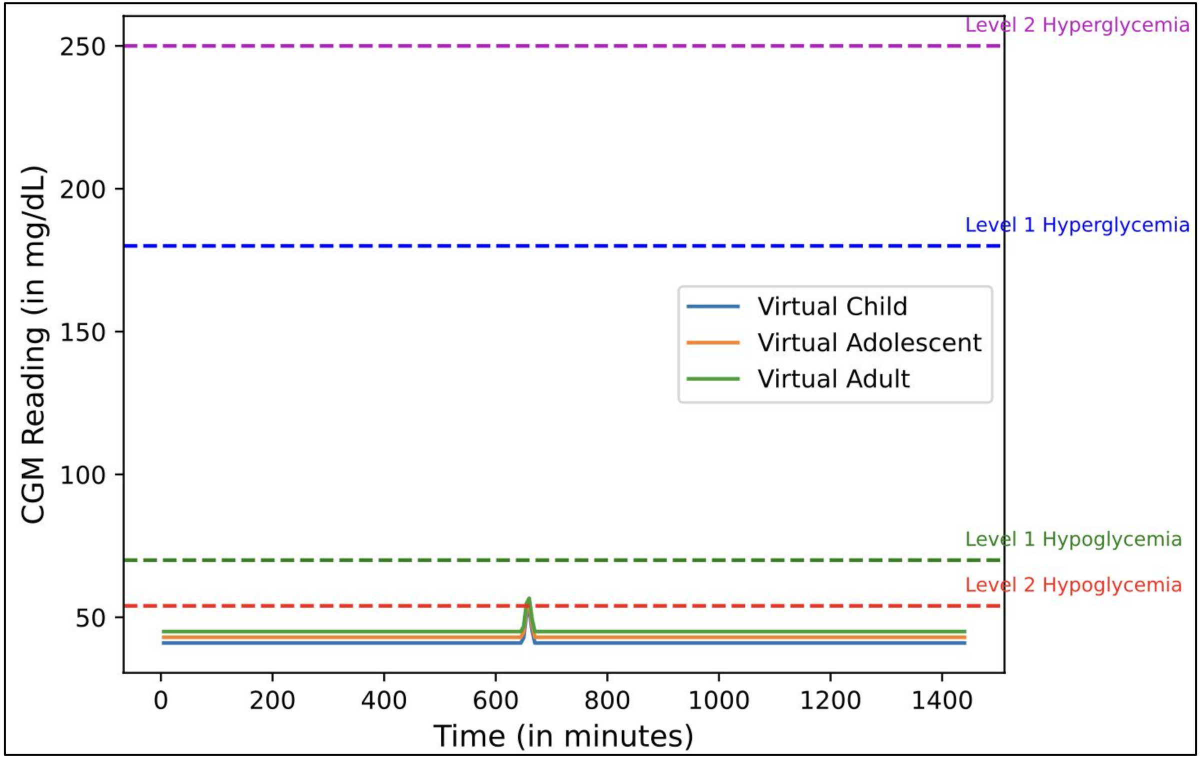
ML security architecture



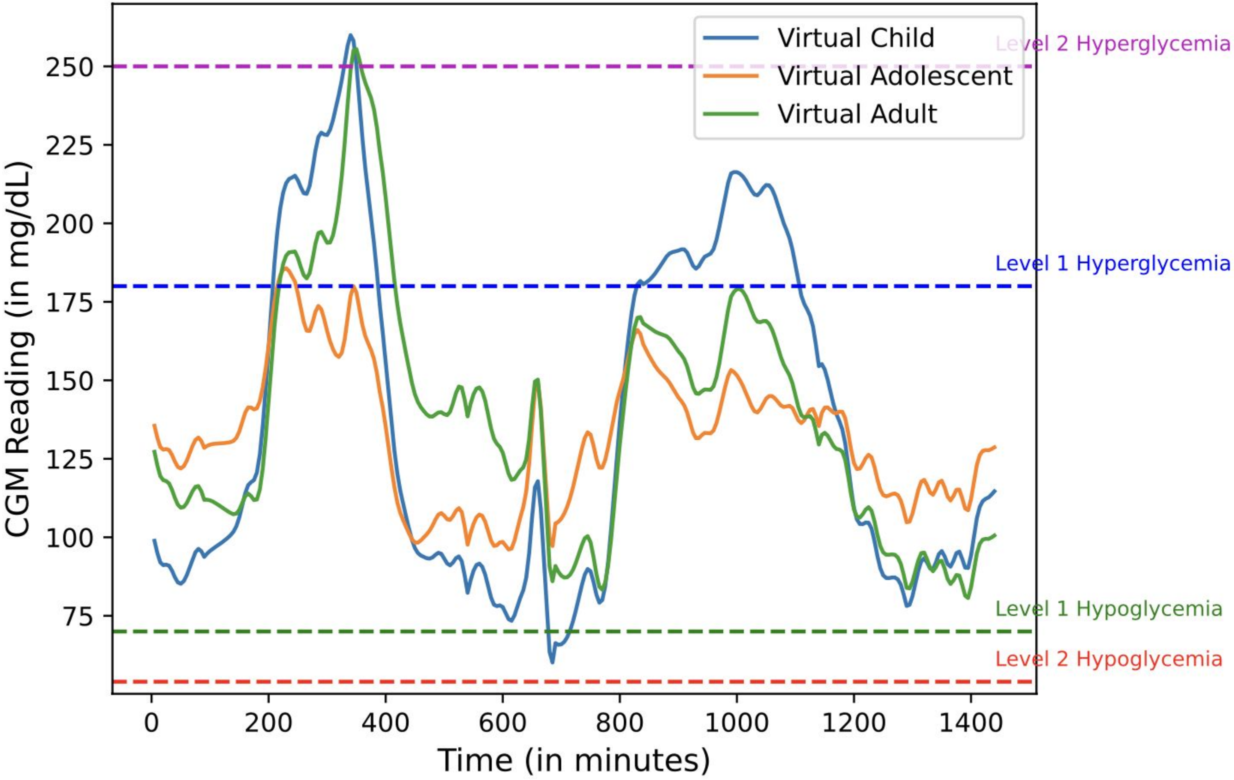
Bound ML predictions with reactive safe model



Malicious model killed several virtual humans

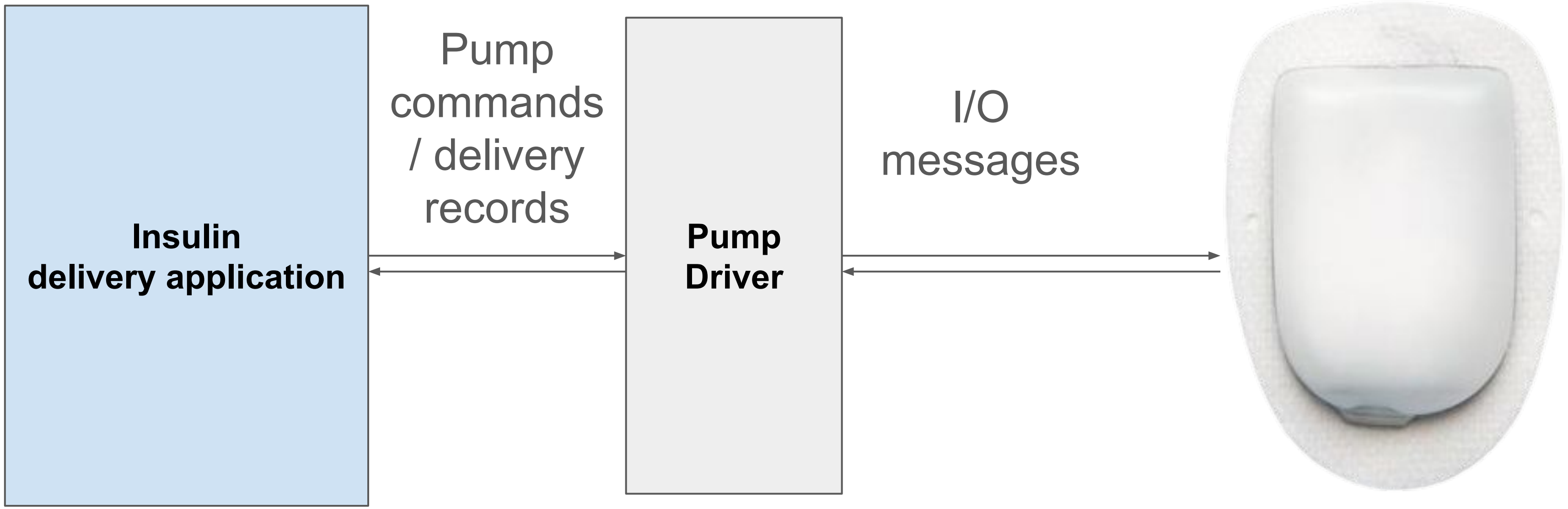


Even with a fully malicious predictive model, GlucOS keeps individuals in range



Driver Security

Insulin pump drivers



Insulin delivery application

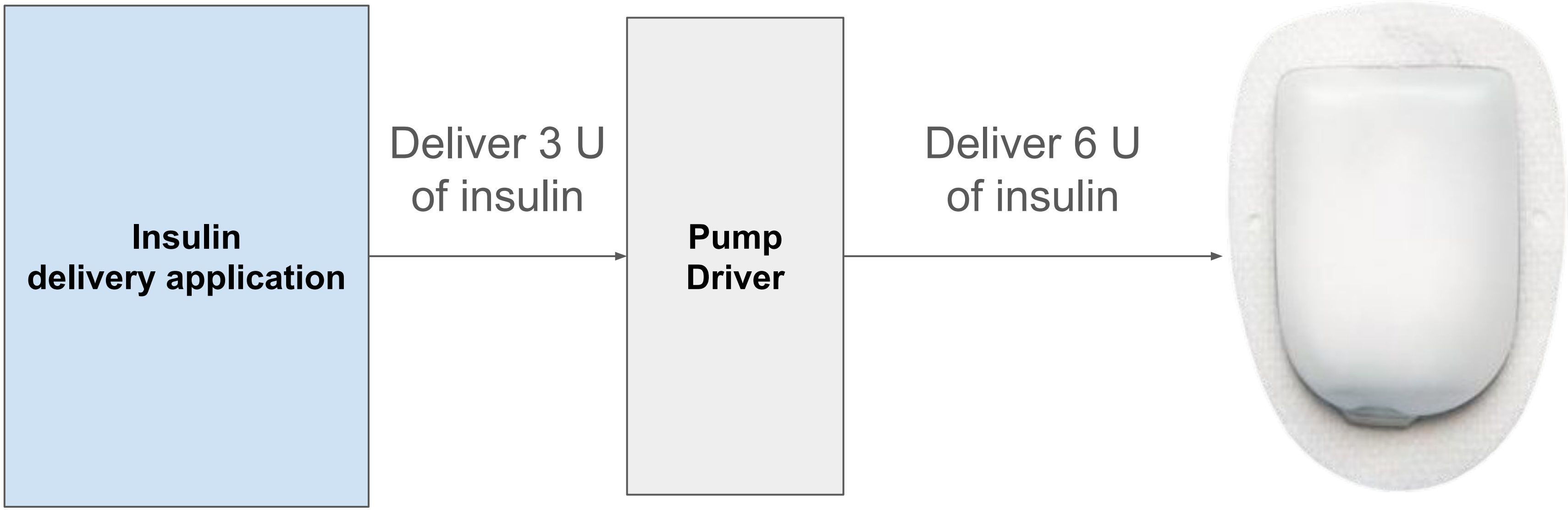
Pump commands / delivery records

Pump Driver

I/O messages

Insulin pump

Buggy / malicious pump drivers



Insulin delivery application

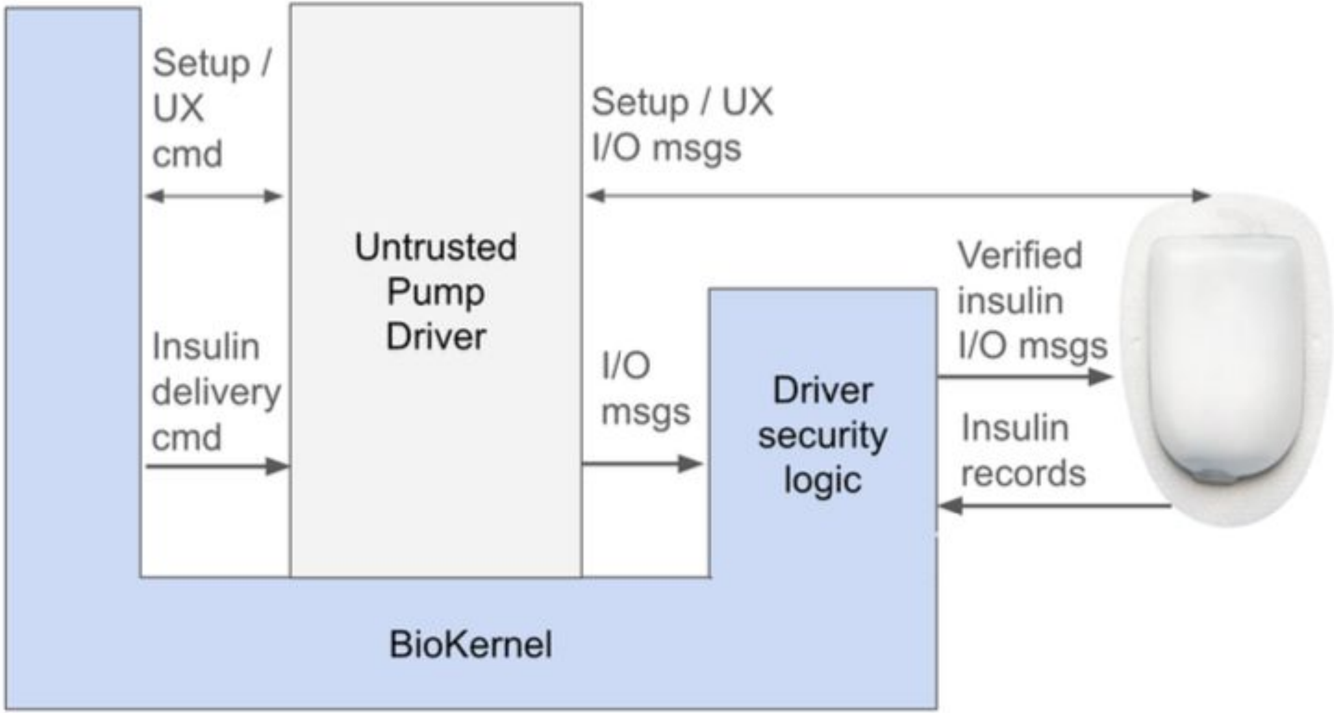
Deliver 3 U of insulin

Pump Driver

Deliver 6 U of insulin

Insulin pump

Driver security mechanism



Simulators do not model pump drivers

End-to-end Security: Biological invariant

Biological invariant

$$|g_{\text{measured}} - g_{\text{predicted}}| < 30\text{mg/dl}$$

Biological invariant

$$\left|g_{\mathsf{measured}} - g_{\mathsf{predicted}}\right| < 30\mathsf{mg/dl}$$

$$\left|g_{\mathsf{measured}} - g_{\mathsf{actual}}\right| < 5\mathsf{mg/dl}$$

Biological invariant

$$\left|g_{\mathsf{measured}} - g_{\mathsf{predicted}}\right| < 30\mathrm{mg/dl}$$

$$\left|g_{\mathsf{measured}} - g_{\mathsf{actual}}\right| < 5\mathrm{mg/dl}$$

$$\left|g_{\mathsf{measured}} - g_{\mathsf{predicted}}\right| < 35\mathrm{mg/dl}$$

Real-world vs. simulation

- Current simulators do not capture fluctuations to insulin sensitivity

- On an individual using GlucOS, we observed violations to the biological invariant occurring 1.6k times over a 2 month period

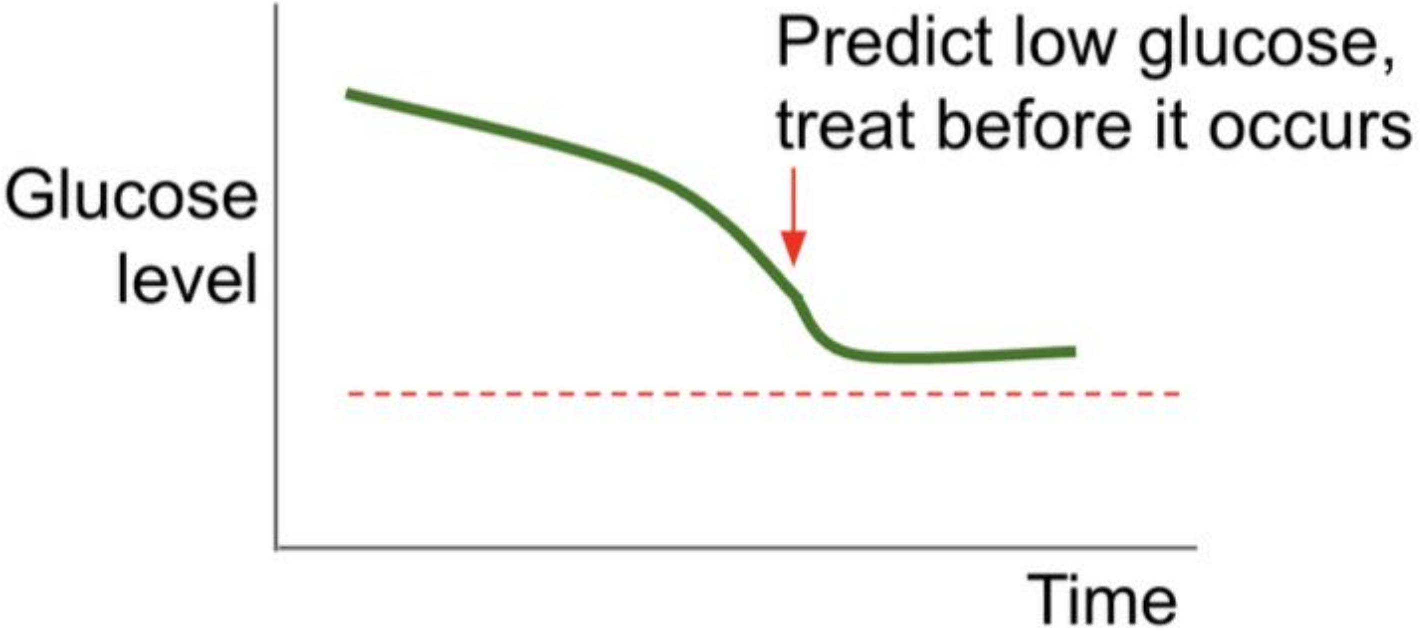
Keeping humans in the loop

Humans form the last level of defense

- Certain situations require humans to intervene

- E.g., humans have to eat food to lift up their glucose levels if they're too low

Predictive alerting and personalization



Should alerting be incorporated within our TCB?

- We initially chose to keep alerting outside our TCB for simplicity
- However, communication channels provided by iOS introduced complications, where individuals did not receive alerts when they lost connectivity
- We incorporate alerting within the TCB in our current implementation but highlight the need for additional communication channels for health

Impact on real humans

- Individual using GlucOS had their tightest ever control
  - Matched that of non-diabetics

- They also faced significantly lower cognitive load

- We also report tighter control across all participants in our user study

- All participants also reported significantly lowered cognitive load

Conclusion

- People with T1D can live longer than their peers

- Biohacking software grounded in security first principles can pave the way for increased longevity for all individuals

Thank you.

Please email your questions to:

hvenugopalan@ucdavis.edu

or

smvijay@ucdavis.edu