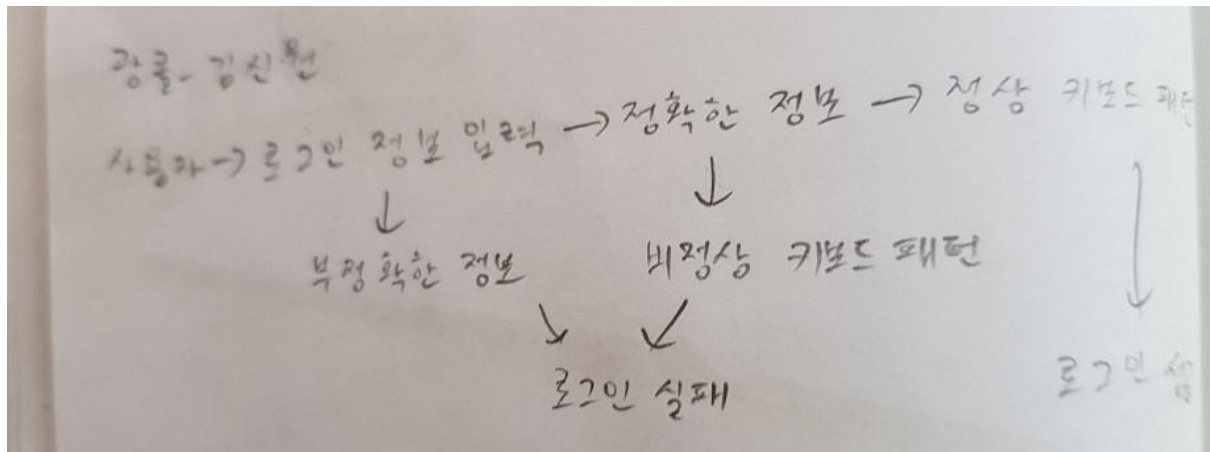


디자인 스프린트1, 2

성명: 김신원

학번: 201701989

1. 문제에 대한 지도 만들기



2. 문제에 대한 질문 만들기

어떻게 하면 정확하게
사용자와 해커를 구분할 수
있을까?

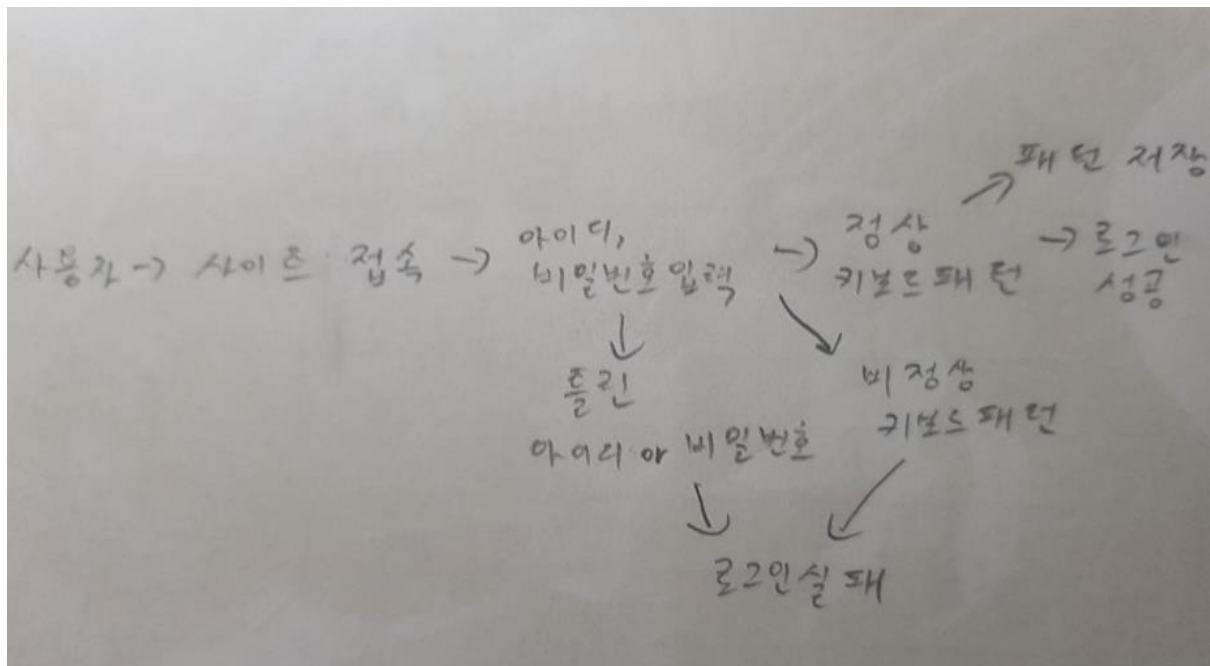
어떻게 하면 키스트로크 다이내믹스
가 쓰였는지 여부를 사용자에게
명시할 수 있을까?

어떻게 하면 최소한의 키보드
밀력으로 사용자와 해커를
구분할 수 있을까?

어떻게 하면 최소한의 시간으로
사용자와 해커를 구분할 수 있을까?

어떻게 하면 사용자가 납득할
수 있는 기준으로 사용자와
해커를 구분할 수 있을까?

3. 합친 map과 hwm



어떻게 하면

최소한의 시간으로
문고만 할 수 있을까?

We Innovate Healthcare

어떻게 하면

보안성을 높일 수 있을까?

We Innovate Healthcare

어떻게 하면

큰그릇창을 한 눈에
갈 보이게 할 수 있을까?

We Innovate Healthcare

여러분께 하련

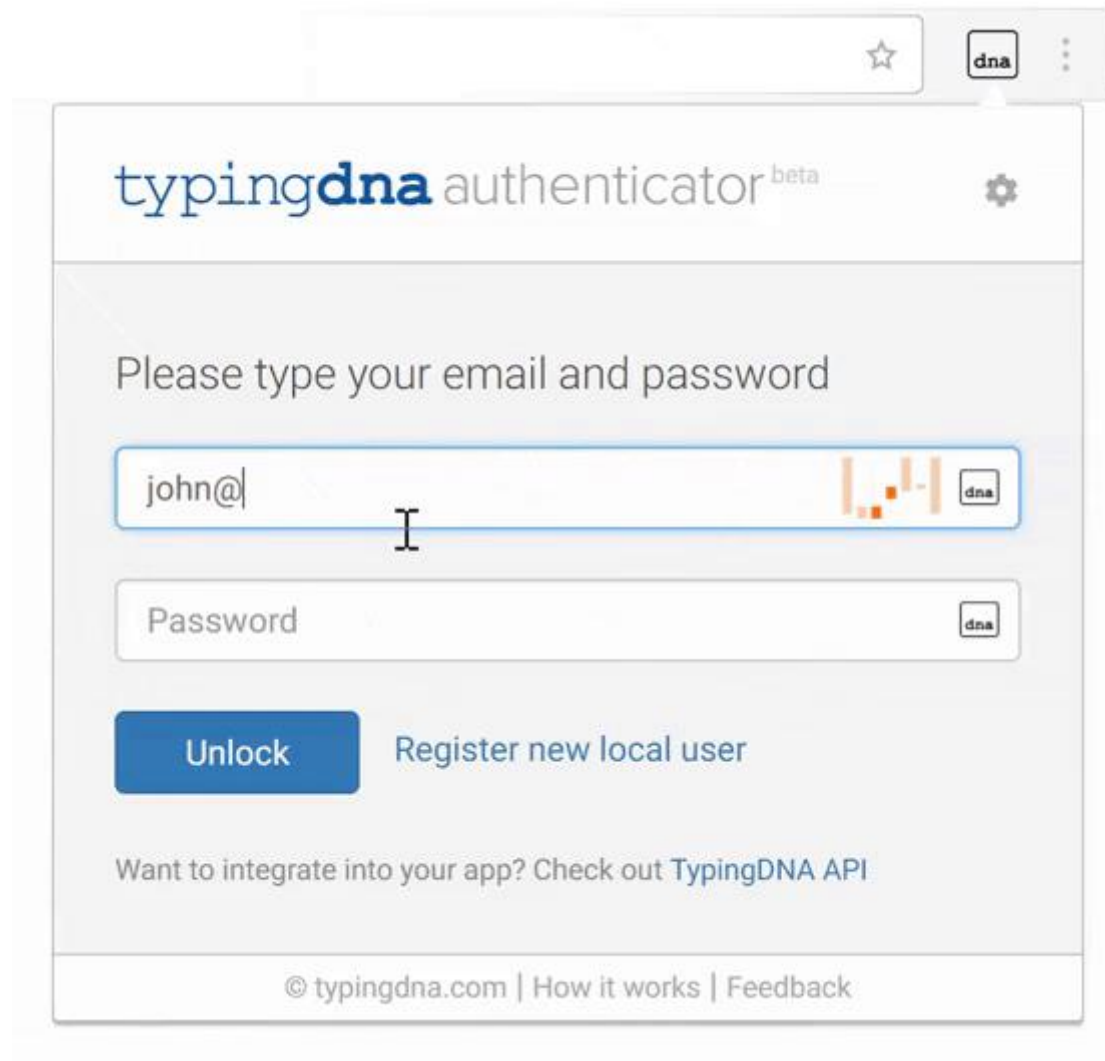
4. 뭘자가 신뢰하게
할 수 있을까?

We Innovate Healthcare

4. Lightning Demo

TypingDNA

<https://www.typingdna.com/>



The image shows a web browser window displaying the TypingDNA Authenticator Beta login page. The browser's address bar is empty, and the page title is "typingdna authenticator^{beta}". The page has a light gray background with a white header area. Below the header, the text "Please type your email and password" is displayed. There are two input fields: the first is for the email, containing "john@" with a cursor, and the second is for the password, labeled "Password". Both fields have a "dna" logo in the top right corner. Below the input fields, there is a blue "Unlock" button and a link "Register new local user". At the bottom, there is a link "Want to integrate into your app? Check out TypingDNA API" and a footer with "© typingdna.com | How it works | Feedback".

typingdna authenticator^{beta}

Please type your email and password

john@

Password

Unlock Register new local user

Want to integrate into your app? Check out [TypingDNA API](#)

© typingdna.com | [How it works](#) | [Feedback](#)

Keystroke DNA

<https://keystrokedna.com/>



HOW you type, not WHAT you type

Keystroke dynamics studies one's behavioral patterns and uses this data for identification purposes, independent of language, words or characters.



Effective on keyboard and keypad

Keystroke DNA can recognize the identity of a user whether they're on a keyboard or a touchscreen as individual typing patterns remain unique.



Simple integration

Keystroke DNA can be easily integrated into any web application with just a few lines of code. It doesn't require any expertise in biometrics.



Resistant to password attacks

Keystroke DNA provides a more secure method of authentication that keeps data secure and access under control even if a password is hacked or stolen.



More reliable

Unlike static biometric authentication methods, Keystroke DNA recognizes dynamic typing patterns, which cannot be shared or imitated.

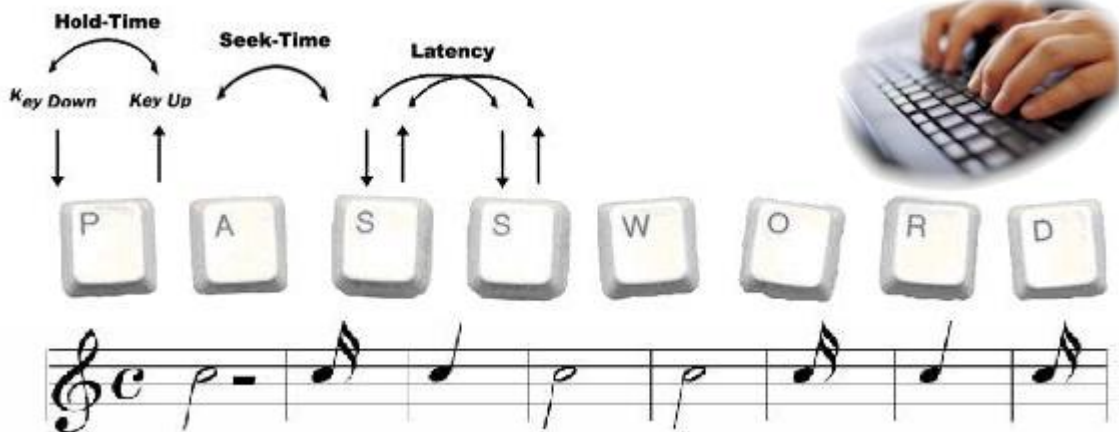


No special hardware required

Keystroke DNA requires only a keyboard or keypad making it the most convenient and affordable method of biometric authentication available.

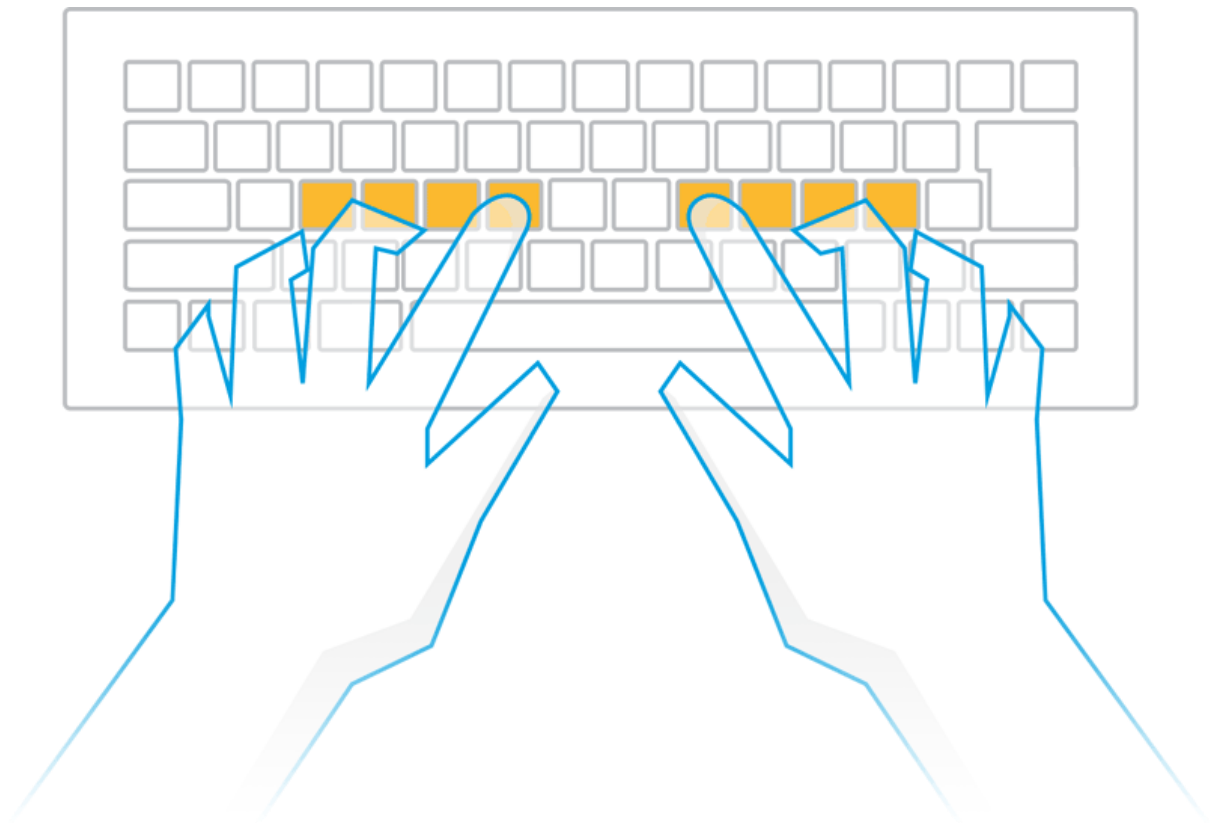
deepnetsecurity

<http://www.deepnetsecurity.com/authenticators/biometrics/typesense/>



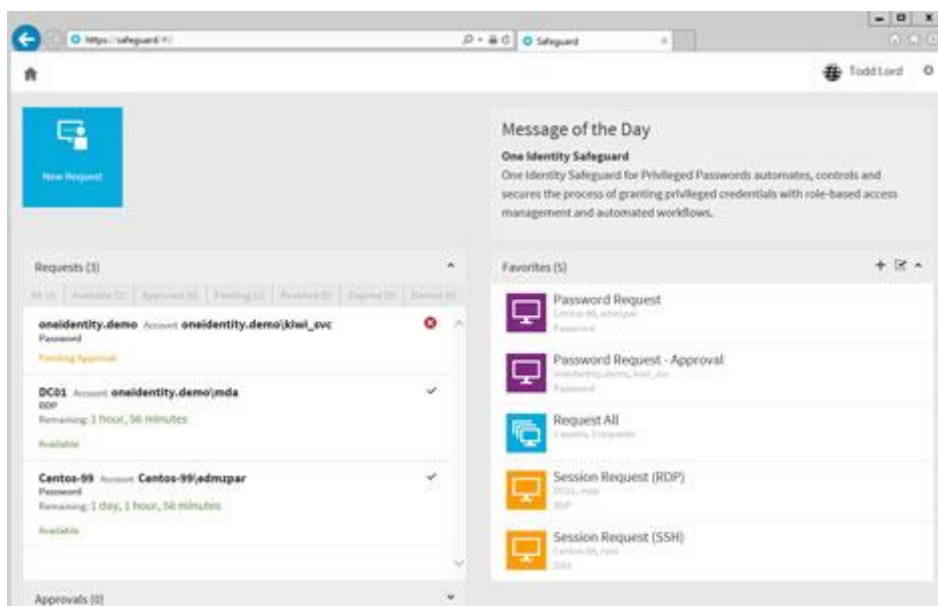
Daon

<https://www.daon.com/biometrics/keystroke>



oneidentity

<https://www.oneidentity.com/one-identity-safeguard/>



keytrac

<https://www.keytrac.net/>

WORKS WITHOUT SPECIAL HARDWARE

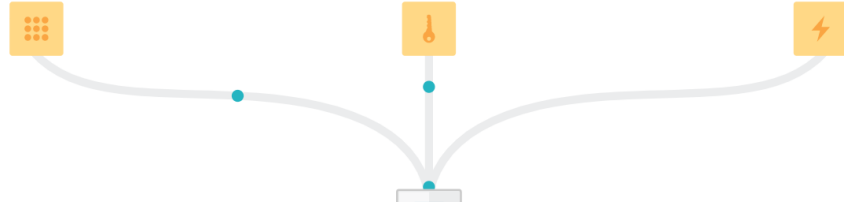
We don't require expensive biometric hardware. KeyTrac works with your existing, ordinary keyboard.

NOTHING TO BE LOST OR STOLEN

Keystroke dynamics is a security feature which can't be lost or stolen. Just type in a short textphrase and you're done.

FAST, RELIABLE AND UNFORGEABLE

KeyTrac grows with your keystroke dynamics and adapts to your typing pattern to remain unforgeable.



5. Crazy8's

