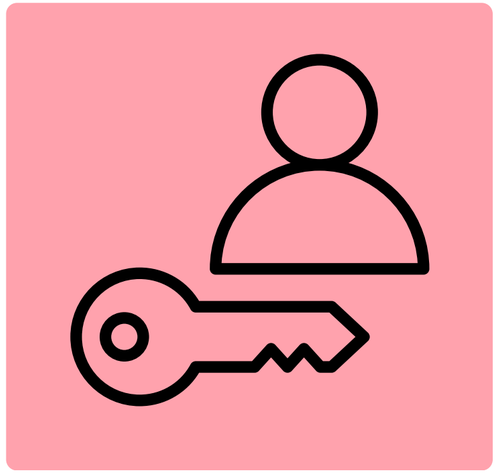
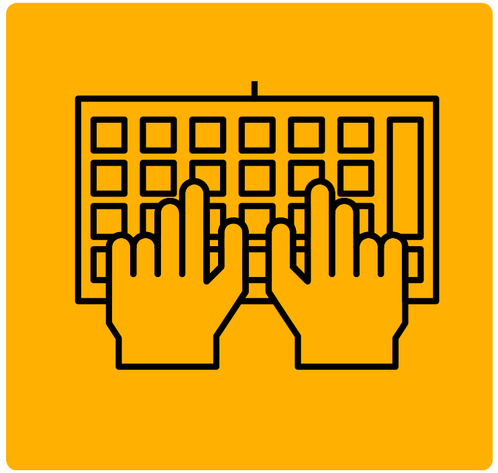
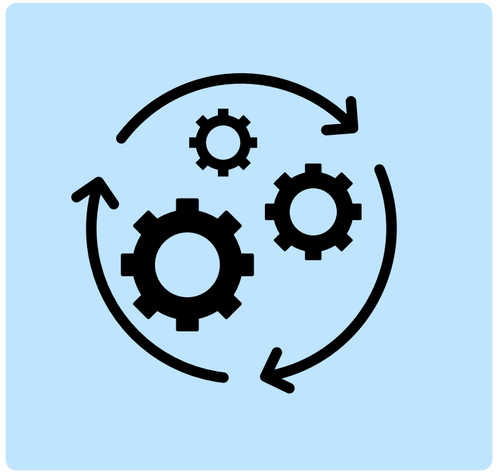
Do Continuous Authentication Products Perform as Advertised in the Real World?

An evaluation of some continuous authentication solutions.





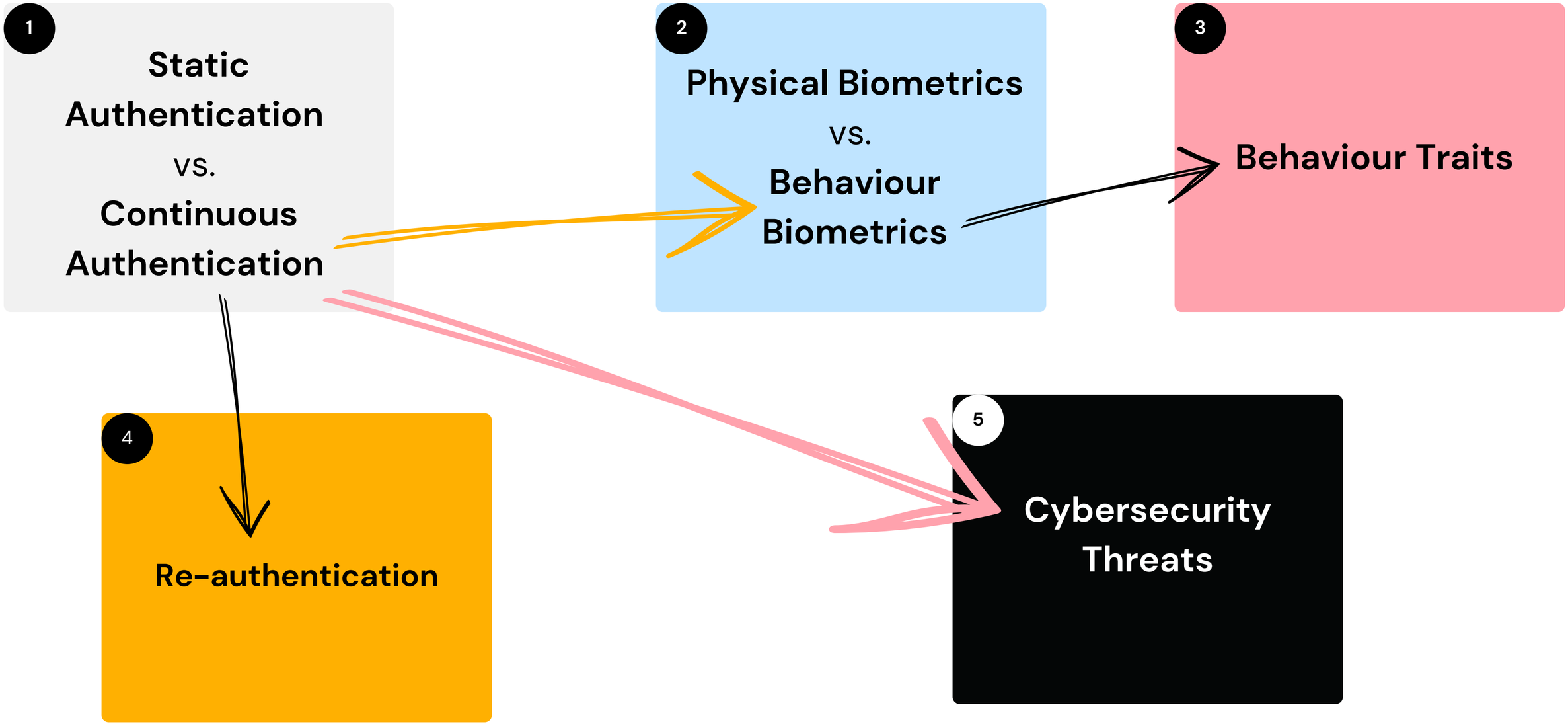


Funmilayo Olaiya
Cheriton School of Computer Science
University of Waterloo

DEC. 5. 2022

Introduction & Background

Deeper into Continuous Authentication



A Simple Concept on how CA works

A particular behaviour biometric trait must be trained on the computer

A user using an authenticated computer

Trying to detect if the user is legit

Another user trying to use the other user's computer

If the user is not legit

Continuous detection of the legit user at whatever intervals

CA Solutions (AaaS) // ZERO-TRUST strategy

PRODUCTS/COMPANIES	SOLUTIONS	SCHEMES	HOW IT WORKS (MECHANISM)	RUNNING PLATFORMS	TARGET MARKET	THREATS
TYPINGDNA	**ActiveLock**	Typing biometrics(keystroke dynamics/biometrics)	Continuous Typing Dynamics	Mac & Windows	Remote Workforce (Work computers)	Identity Theft (Device)
BEHAVIOSEC	-----	Typing & Mouse Dynamics	Integration with platform // Scores data from day 1	Installs as a software components on-premises	Enterprises/Businesses/Financial solutions	Account Takeover
SECUREAUTH	**Arculix**	Patterned behaviour modelling	Continuous passwordless authentication	Mobile/desktop/cloud/web/systems	Businesses	Reduce fraud /Account Takeover
ZIGHRA	----- **Continuous MFA**	Device type, location details, with Behaviour biometrics; type, touch & hold	Integration with platform // Continuous mentioned systems to start scoring data	Mobile/desktops	Remote workforce and customers	Remote Attacks & Account Takeover
NUDATA SECURITY	**NuDetect**	Device intelligence/ Behavioural analytics / Passive behaviour biometrics / Behavioural Consortium	Integration with platform	Mobile / Desktops / Web	Businesses	Reduce fraud

Related Work

Related Work

1. Behavioural Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective
   By Liang et al.

2. User authentication through typing biometrics features.
   By Araújo et al.

3. Spoof Attacks on Gait Authentication System.
   By Gafurov et al.

Methodology

TypingDNA as a Case Study

typingdna

- Why TypingDNA? - Available, Accessible, Interesting, Popular

What are the advertisements?

- They mentioned that it's **foolishness** to use your work laptop for other activities.
- ZERO-TRUST strategy // No device sharing

A little bit on *Keypad Biometrics* a.ka. Typing Biometrics

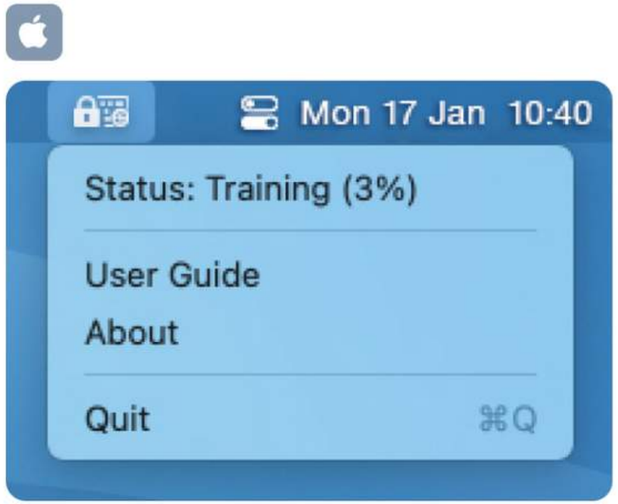
1. ***According to Biometrics Solutions*** - Keystroke dynamics or typing biometrics - an automated method of identifying or confirming the identity of an individual based on the manner and the rhythm of typing on a keyboard.

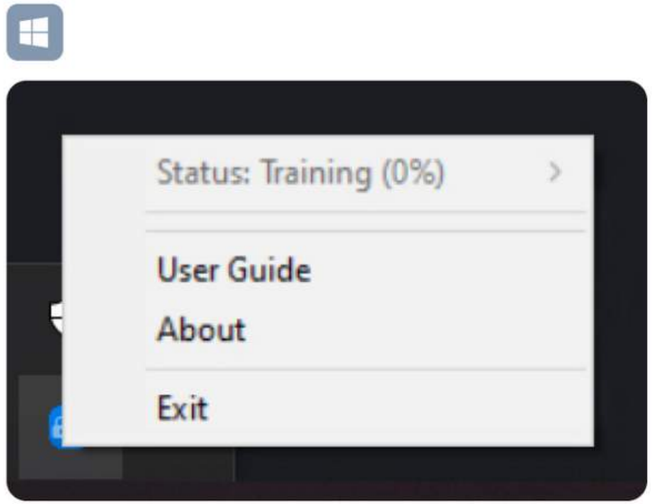
2. Dwell time - time duration that a key is pressed - Key Down
   Flight time - time duration between releasing a key (Key Up) and pressing the next key (Key Down)

Credit: https://owasp.org/www-pdf-archive//Ksd.pdf

Accessing TypingDNA

- Download & Train - Type about 2000 words with 1/2 days or extended



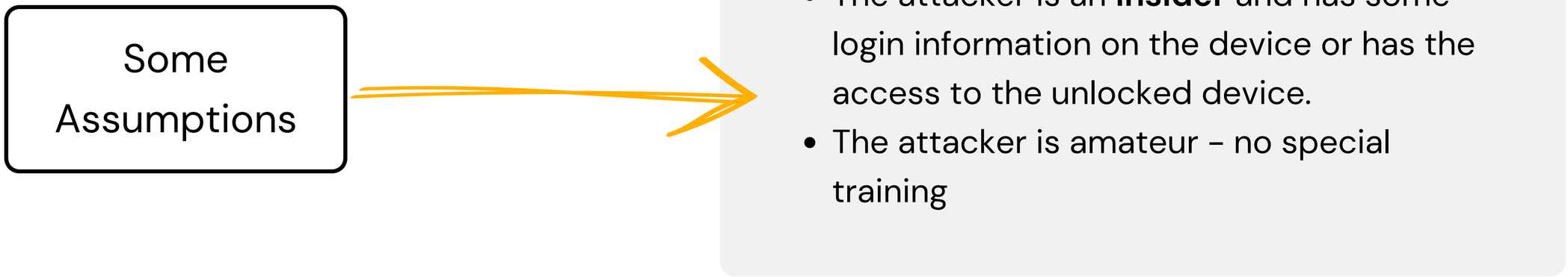


- **Less restrictive**: optimized for better user experience, with minimal disruptions for a genuine user
- **Balanced**: the recommended setting and the perfect balance between security and user experience
- **More secure**: increased security but higher chances of false rejection

From TypingDNA

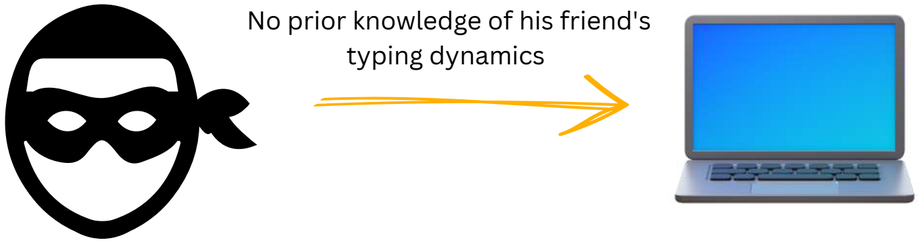
Threat Model

- Gafurov's Spoofing Experiment. PhD. Dissertation - **Performance and Security Analysis of Gait-based User Authentication** (2008) and his Paper**: Spoof Attacks on Gait Authentication System** (2007)

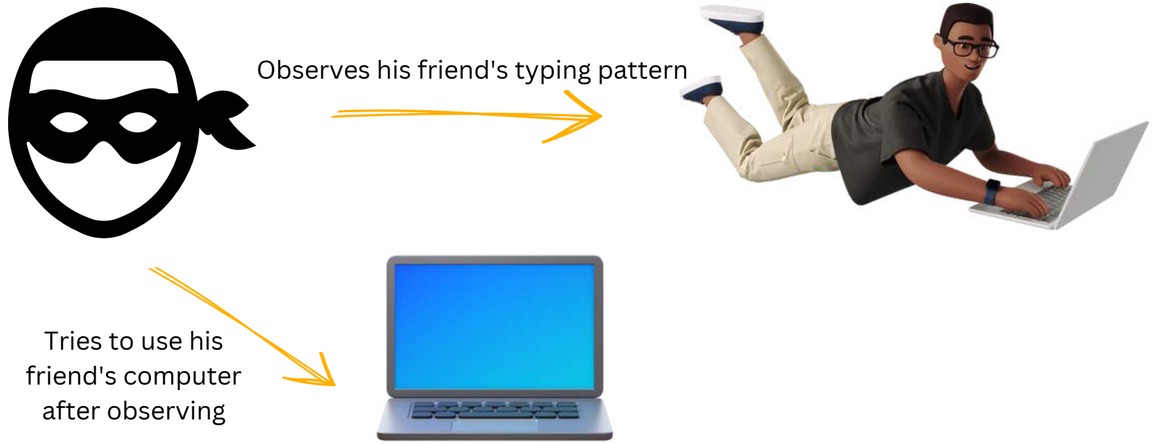


Attack Simulations

Attack Simulation 1 - Impostor



Attack Simulation 2 - Observer Impostor



Results

TypingDNA did not detect the impostor really fast

About the impostor

- Relationship, motivation, background, no special training, time

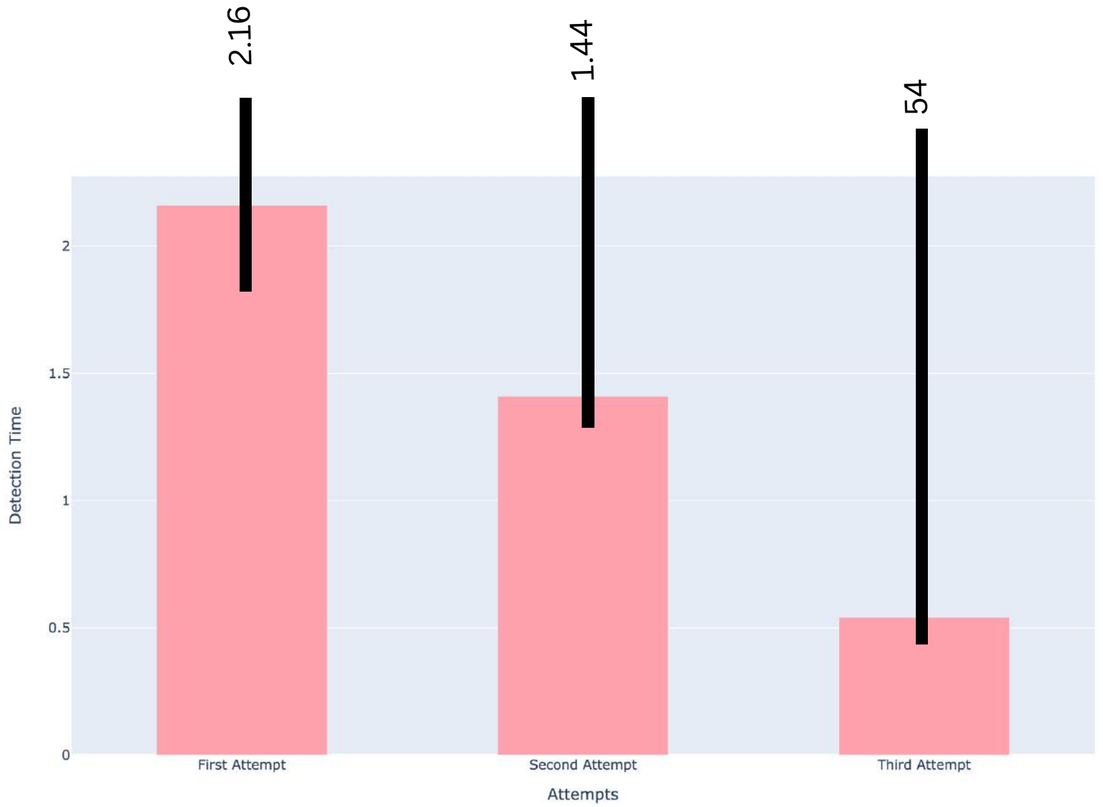
Original template of words

Squire Trelawney, Dr. Livesey, and the rest of these gentlemen having asked me to write down the whole particulars about Treasure Island, from the beginning to the end, keeping nothing back but the bearings of the island, and that only because there is still treasure not yet lifted, I take up my pen in the year of grace 17–, and go back to the time when my father kept the "Admiral Benbow" inn, and the brown old seaman, with the sabre cut, first took up his lodging under our roof.

I remember him as if it were yesterday, as he came plodding to the inn door, his sea-chest following behind him in a hand-barrow; a tall, strong, heavy, nut-brown man; his tarry pigtail falling over the shoulders of his soiled blue coat; his hands ragged and scarred, with black, broken nails; and the sabre cut across one cheek, a dirty, livid white. I remember him looking round the cove and whistling to himself as he did so, and then breaking out in that old sea-song that he sang so often afterwards:–

181 Words

- First attempt – 102 words
- Second attempt – 77 words
- Third attempt – 37 words



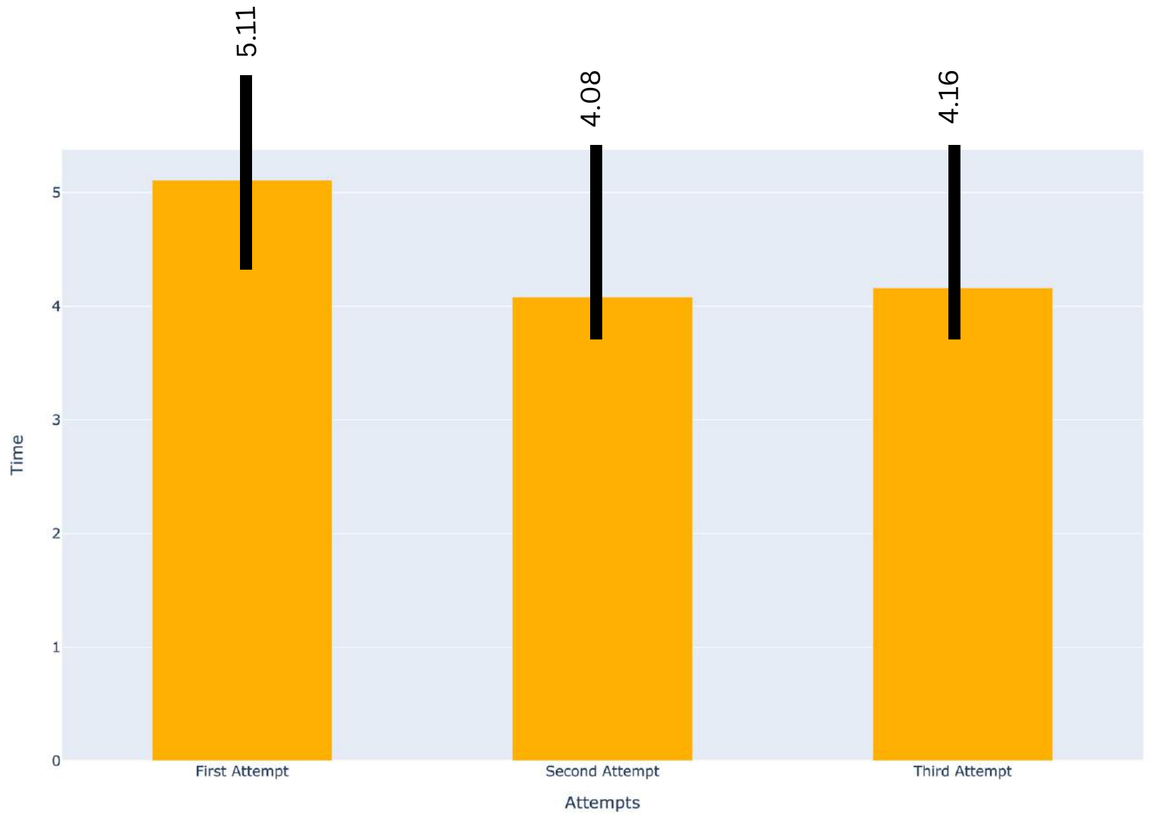
TypingDNA did not detect the observer impostor at all

What the attacker observed during a friendly chat:

Observation 1:
Right hand - middle finger, Thumb - space bar
Left hand - index finger, no other finger
Speed - pretty fast

Observation 2:
Speed - pretty faster
Making sure hands are placed like the victim's own

Observation 3:
Left hand - thumb to press commands like caps lock, shift keys, etc



- First attempt – 181 words
- Second attempt – 181 words
- Third attempt – 181 words

Did TypingDNA satisfy the conditions of the continuous cycle? – Partially

ATTACKS	FIRST ATTEMPT	SECOND ATTEMPT	THIRD ATTEMPT
IMPOSTOR	SUCCESS	SUCCESS	SUCCESS
OBSERVER IMPOSTOR	FAILURE	FAILURE	FAILURE

- **Note**: TypingDNA was only able to detect an "**ordinary impostor**".

Did TypingDNA recognize other forms of activity apart from typing? - No

ATTACKS	FIRST ATTEMPT	SECOND ATTEMPT	THIRD ATTEMPT
IMPOSTOR	FAILURE	FAILURE	FAILURE
OBSERVER IMPOSTOR	FAILURE	FAILURE	FAILURE

- **Note**: The attacker browsed, watched youtube videos, and opened my email account for as long as she wanted.
- *There was no definite amount of time, but we made sure it was about a few minutes longer than the time it took for TypingDNA to recognize the imposter's 3rd attempt.*

Did TypingDNA identify the impostor's typing biometrics when she signed into the device? - No

ATTACKS	FIRST ATTEMPT	SECOND ATTEMPT	THIRD ATTEMPT
IMPOSTOR	FAILURE	FAILURE	FAILURE
OBSERVER IMPOSTOR	FAILURE	FAILURE	FAILURE

- What if the impostor had some login information?

On TypingDNA's Accuracy

Error rates used in calculating the accuracy of a biometric system

1. False Acceptance Rate (FAR)

$$FAR = \frac{Number\ of\ accepted\ impostor\ attempts}{Total\ number\ of\ impostor\ attempts}$$

= 1

2. False Rejection Rate (FAR)

$$FRR = \frac{Number\ of\ rejected\ genuine\ attempts}{Total\ number\ of\ genuine\ attempts}$$

= 0

3. Equal Error Rate

$$EER = \frac{FAR + FRR}{2}$$

= 0.5 / 0

Challenges & Limitations

1. Tight companies

2. No strong body of work yet on the evaluation of CA solutions

3. Finding the right kind of attack model, *but later got something at the end*!

Future Work (What can be done next?)

1. Simulating an injury to see if it still detects a legitimate user; because TypingDNA mentioned –
   - *if the typing pattern of a user has changed drastically due to an injury. The best course of action is to reset the training.*
2. Evaluating other CA solutions; especially related to mouse dynamics – **Behaviosec**
3. Several other attempts with many participants as victims & attackers to evaluate different results
4. Simulating a different form of attack – A different threat model ~ extracting the typing pattern of a victim from a compromised biometrics dataset

Key Takeaways & Conclusion

1. If TypingDNA had combined "Mouse Dynamics" with their "Typing Biometrics" system, it could have made for a stronger product

2. Detection Speed was quite low for the impostor - serious damage could have been done within this time frame

3. It would have been great if TypingDNA recognised the typing biometrics of the impostor upon signing in back. But it did not!

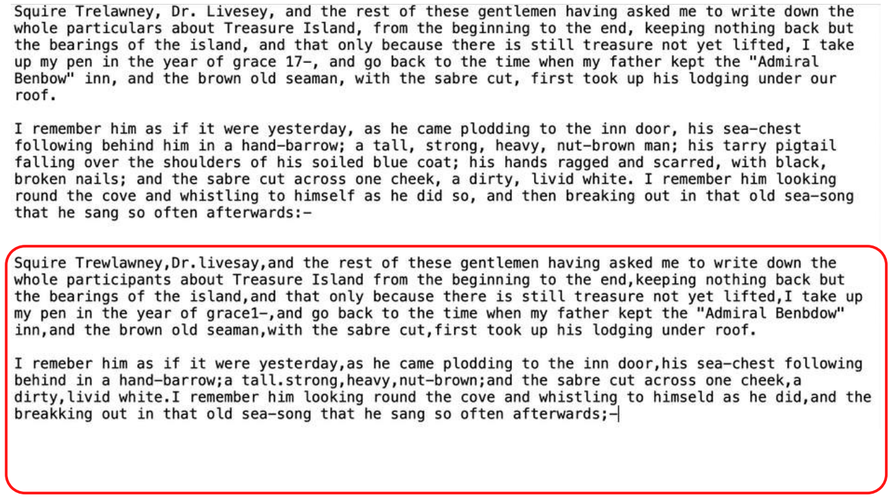
Appendix

An example of what the observer Imposter typed

Squire Trelawney, Dr. Livesey, and the rest of these gentlemen having asked me to write down the whole particulars about Treasure Island, from the beginning to the end, keeping nothing back but the bearings of the island, and that only because there is still treasure not yet lifted, I take up my pen in the year of grace 17–, and go back to the time when my father kept the "Admiral Benbow" inn, and the brown old seaman, with the sabre cut, first took up his lodging under our roof.

I remember him as if it were yesterday, as he came plodding to the inn door, his sea-chest following behind him in a hand-barrow; a tall, strong, heavy, nut-brown man; his tarry pigtail falling over the shoulders of his soiled blue coat; his hands ragged and scarred, with black, broken nails; and the sabre cut across one cheek, a dirty, livid white. I remember him looking round the cove and whistling to himself as he did so, and then breaking out in that old sea-song that he sang so often afterwards:–

181 Words



First attempt