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

Funmilayo Olaiya
Cheriton School of Computer Science
University of Waterloo
folaiya@uwaterloo.ca

ABSTRACT

The continuous authentication solutions provided by a few companies are looked at in this research as one from a particular company is evaluated. Using TypingDNA as a case study, we carefully examine the solution marketed by this company called - **ActiveLock**. TypingDNA's ActiveLock solution was simple to analyze because the company provides a complimentary licence that users can freely use to download and evaluate the desktop app. We made sure to download the app on a computer owned by a specific individual because ActiveLock requires users to have their typing dynamics trained on their own computers. The individual had to type about 2000 words over the course of a few days to train the app. After the training, we looked at two primary instances where an impostor and an observer impostor try to type about 181 words on the computer because we wanted to test the app to determine whether it could truly identify the impostors. Our findings indicate that, for the impostor, it took the app a significant length of time before it recognised and logged the impostor out, but that after the initial attempt, the duration gradually decreased. In addition, the app did not detect the observer impostor in any of the attempts and did not log the impostor out at all. Furthermore, we were unable to identify whether this was a result of TypingDNA's implementation of ActiveLock, the security level of ActiveLock or a well-known drawback of keystroke dynamics which is—poor accuracy.

KEYWORDS

continuous authentication, authentication, behaviour biometrics, keystroke dynamics, typing biometrics, typingdna

1 INTRODUCTION

Over the past several years, continuous authentication technology has been increasingly popular and in demand. The primary objective of this method of authentication is to essentially address the drawbacks of static authentication and propose novel techniques for elevating a user's mode of authentication in terms of enhanced security and usability (user experience).

For many years and up until today, static authentication has been the usual way of authentication, particularly when using common authentication techniques like pins, passwords, and some physical biometric techniques like touch id (fingerprint recognition) and face id (facial recognition). On the other hand, continuous authentication is a type of authentication that leans toward continuously confirming the identity of a user who has already been authenticated [12]. Web sessions are frequently employed in many web platforms for re-authentication purposes. However, this approach has been shown to seriously worsen user experience, as frequent logging in and out causes the user great stress [12]. As a solution to the necessity for re-authentication, continuous authentication is becoming more desired.

Currently, many different startups offer customers continuous authentication (CA) solutions, with businesses serving as their primary target market. In this paper, we will look at a few of these solutions and use one of them called ActiveLock by TypingDNA as a case study. For ActiveLock-we want to assess how this solution works, how it is used and enabled, what purpose it actually serves, and most significantly, if it truly works.

The term **behavioural biometrics** describes the distinctive behavioural characteristics that can be used to authenticate people [11]. Behavioural biometrics, as opposed to static authentication techniques or physical biometrics, uses a user's behaviour to identify them [11]. Many of the present CA solutions heavily rely on behaviour biometrics, including gait, keyboard, mouse dynamics, and many more.

Behaviour biometrics has been a popular choice of technique for CA solutions since it is considered to be secure, inexpensive, impossible to steal, difficult to copy, and continuous because as a factor of authentication-it is *something you do*.

In this paper, we carefully evaluate the **ActiveLock by TypingDNA** [1] solution and try to conduct spoofing attacks against it. Keystroke dynamics, often known as *typing biometrics*, is the principal behavioural biometric technique used by ActiveLock. Setting up ActiveLock was quite simple because all we had to do was download the desktop application and type roughly 2000 words to train it on how to recognise the typing pattern of the user *(the owner of the computer that ActiveLock was downloaded to)*.

We also employed two attack simulations: one involving an **impostor** who is just acting normally and trying to use the computer, and another impostor, called **observer impostor**-who has actually observed the victim's typing style and also tries to use the victim's computer.

Our study demonstrated that ActiveLock may have detected the impostor but failed to act quickly enough on the initial attempt, while ActiveLock was completely unable to identify the observer impostor in all attempts.

We make the following contributions;

- Finding businesses that offer CA solutions to users and assessing them according to various use cases.

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

- Using ActiveLock from TypingDNA as a case study to ascertain whether it truly performs as advertised.
- Performing spoofing attacks through imitation experiments to evaluate ActiveLock's security accuracy.

2 BACKGROUND

In this section, we give a quick overview of some background information related to this study.

2.0.1 Behaviour Biometrics. For numerous startups that provide CA solutions, behaviour biometrics has been shown to be quite beneficial. The CA solutions we found all make use of behaviour biometrics or pair it with another type of intelligence. The main justification for this is that behaviour biometrics can continuously ensure authentication without significantly compromising a specific user's usability or user experience.

Behavioural biometrics are categorised as **something you do**-as an authentication factor. Therefore, a user only needs to continue being themselves while they remain continuously authenticated. Another important factor is that no external hardware is really required; instead, a user simply uses what is already in place, like a keyboard [2].

2.0.2 Keystroke Dynamics. Keystroke dynamics, a type of behavioural biometrics, is an automated way of determining a person's identity based on the manner and rhythm in which they type on a keyboard [13]. Metrics like **Dwell time** and **Flight time** are utilised to measure keystroke dynamics. Dwell time refers to the length of time a key is pressed, and flight time is the time interval between keystrokes (releasing a key and pressing the next key) [13].

Keystroke dynamics is thought to be non-intrusive, distinctive, and has a minimal implementation cost, but some of its drawbacks include the possibility of low accuracy [3]. The primary biometric method used by ActiveLock-the solution we will use as a case study is keystroke dynamics.

2.0.3 Machine Learning. Artificial intelligence (AI), behavioural biometrics, and machine learning (ML) all work hand in hand [14] to deliver interesting and intelligent solutions. Because ML is adaptable and has the capacity to continuously learn from human behaviour, ML is used in all types of behavioural biometrics implementation [14].

2.0.4 Continuous Authentication Solutions. Nowadays, some companies, particularly those in the finance industry, rely on CA solutions to reduce the fraud rate. And many startups, which we shall look at in a later part, make the claim to offer solutions that help to lower the risk of fraud.

Businesses are these companies' preferred target market, which may be because the majority of cybersecurity threats that the CA solutions are designed to address are more prevalent in organisations with authenticated employees, numerous users or customers, or businesses that deal with money on a regular basis.

2.0.5 Cybersecurity Threats. Many organisations in the real world are victims of highly frequent cyberattacks such as Account Takeover (ATO), Phishing, Brute-force, Insider threats, Fraud, and many others. There are a number of CA companies out there that claim their solutions mitigate most of these threats.

3 RELATED WORK

There hasn't really been any major research on evaluating CA solutions offered by startups. Although this study proves itself as the first, and we examine prior research and studies related to this area of research here.

Liang et al. [11] extensively investigated and provided valuable insight into behaviour biometrics with regard to ongoing user authentication. This body of work offered more in-depth explanations for why behavioural biometrics is favoured for CA. It investigates the types of behavioural traits that are chosen for behaviour biometrics systems and how Artificial Intelligence (AI) enters the picture.

Araujo et al. [9] centered their research and study primarily on typing biometrics using a conventional keyboard. Seven experiments were conducted using a combination of approximately four typing biometric features that were measured. Three different users—the legitimate user, the impostor, and the observer impostor—were used to evaluate the experiments of the research. Our research into how to categorise users for our attack simulations was inspired by this study's classification of users.

Gafurov et al. [10] research is focused on trying to establish a minimal type of impersonation attacks on gait biometrics because there haven't been any attacks to test the vulnerability of gait before. They also proved that attackers with knowledge of a very close person can be a serious threat to gait authentication.

4 METHODOLOGY

4.1 Exploring some CA solutions

Our initial step in the research process was to compile a list of legitimate businesses that really offer CA products; which are TypingDNA [4], BehavioSec [5], SecureAuth [6], Zighra [7] and Nudata Security [8]. We discovered about five really interesting businesses that, while providing the same function, do so in various ways. They use a variety of behavioural biometrics or a combination of some, and some of these businesses have a specific name for their solution since they also market other products, such as TypingDNA, while others, like BehavioSec, are primarily CA companies.

These solutions can be used in a variety of ways, either by downloading them or integrating them with a platform. Table 1 shows an overview of some interesting companies that provide CA solutions.

4.2 ActiveLock by TypingDNA as a case study

We encountered a number of challenges when conducting this research, particularly when attempting to obtain demos or SDKs from companies that provide CA solutions. Because TypingDNA's demo was easily available, free, and had a limited licence, we were able to use it as a case study.

We installed TypingDNA on a specific computer (MacBook Pro 13-inch, 2020, 8gb of RAM and macOS Monterey version 12.6), and before ActiveLock could be activated, the computer's owner had to type around 2000 words over the course of a few days. As a result, ActiveLock was trained to learn the owner's typing style while the app was in **Training Mode** shown in Figure 1a and gotten from [4]. When the app had finished its training, as shown in Figure 1b, the

Companies	Solutions	Schemes	How it Works (Mechanism)	Running Platforms	Target Market	Threats
TypingDNA	ActiveLock	Keystroke dynamics/Typing biometrics	Continuous Typing Dynamics	Desktops/Computers	Remote Workforce	Identity theft
BehavioSec	—	Mouse/Typing dynamics	Continuous Mouse/Typing Dynamics	Web/Cloud	Businesses (financial)	Account Takeover/Fraud
SecureAuth	Arculix	Patterned Behaviour Modelling	Continuous Passwordless Authentication	Web and most Devices	Businesses	Fraud/Account Takeover
Zighra	—	Device Type-/Location details with Behaviour Biometrics	Continuous MFA	Mobile/desktops	Remote Workforce and Customers	Remote Attacks/Account Takeover
Nudata Security	Nudetect	Device Intelligence/ Behavioural Analytics/Passive Behaviour Biometrics/Behavioural Consortium	Continuous mentioned Schemes	Mobile/Desktops/Web	Businesses	Fraud

Table 1: Overview of some continuous authentication solutions provided by some startups.

status of the app immediately switched to **Active Mode**, meaning it was ready to detect unauthorised users of that specific computer and ready for usage.

Figure 1b shows that the security level chosen was **Balanced (Recommended)**. This level of security was automatically chosen for us because the version of ActiveLock we were testing had a free and limited licence, so we were unable to select a different level. Additionally, TypingDNA suggests this security level since they consider that selecting the **More Secure** security level may increase security, but might also increase the likelihood of *false rejections*.

Sharing of devices was strongly discouraged in the advertisements TypingDNA ran for ActiveLock on their webpage [1]. Additionally, they mentioned that it is best to keep personal PCs and work computers separate. If you enable ActiveLock on your work computer, no one will be able to use it if they decide to use it.

4.3 Threat model

Our chosen threat model is not strict. We made the assumption that the attacker (the impostor) was an insider—someone who could pass for at least somewhat of a relative or friend of the victim (owner of the computer). Additionally, we assume that the attacker (the impostor) is near the victim while the victim is using the device or has access to the victim's device (computer) by either having some login information or just the unlocked device.
The attacker has no specialised training and is basically an amateur.

Furthermore, because the ActiveLock app has been trained on the owner's typing dynamics, the owner of the computer (on which ActiveLock was downloaded) will act as the victim.

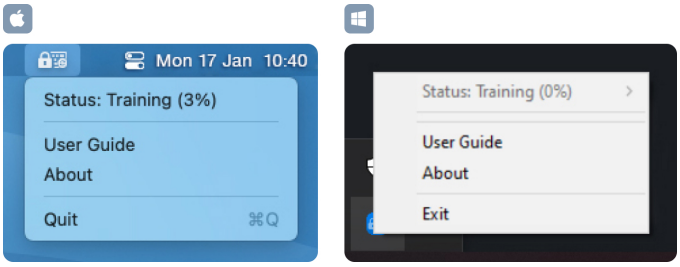
4.4 Attack simulations

We used two different types of attack simulations, and the design of these simulations was influenced by the paper [9] by Araujo et al. The attacker will make three attempts to access the computer while taking on the roles of both an **observer impostor** and an **impostor**.

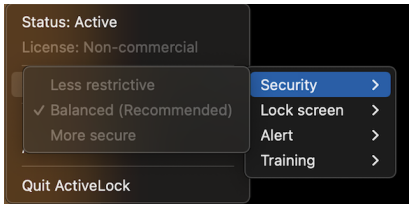
The attacker will play the role of an impostor in the first attack scenario. The impostor has no prior knowledge of the victim's typing dynamics and is given a number of words to type. The impostor will attempt to type these words on the victim's computer three times so as to see how ActiveLock responds to the unauthorised access each time.

The attacker will pretend to be an observer imposter in the second attack scenario. First, the legitimate user will attempt to type the number of words each time before an observer impostor attempts to type the number of words. As a result, the attacker will be able to observe the victim's typing dynamics at various intervals.

The number of words provided to the impostor was 181 as shown in Figure 2.



(a) ActiveLock by TypingDNA in training mode.



(b) ActiveLock by TypingDNA in active mode.

Figure 1: ActiveLock by TypingDNA in various modes.

```
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:—
```

Figure 2: Number of words provided to the impostor.

5 EVALUATION AND RESULTS

Here, we discuss the results of our study and evaluation of ActiveLock.

5.1 ActiveLock detected the impostor, but not quickly

The impostor attempted to type the number of words (181 words) three times, and by using a stopwatch, we calculated the amount of time it took ActiveLock to detect the impostor for each trying time.

What we noticed is that in the first attempt, ActiveLock took a long time before it could detect the impostor but the time steadily decreased following the first attempt as shown in Figure 3. Before ActiveLock could detect, the impostor typed approximately 102 words in the first attempt, 77 words in the second, and 37 words in the third.

5.2 ActiveLock never detected the observer impostor.

Here, the legitimate user (the victim and computer owner) typed exactly 181 words in order to show the imposter observer (attacker) her typing dynamics. This process was carried out in advance of any attack attempts.

In the initial observation, the impostor saw that the victim (legitimate user) types with her left index finger, right middle finger, and right thumb-which is used for a space bar. The observations were correct except that of the *right thumb for space bar.*

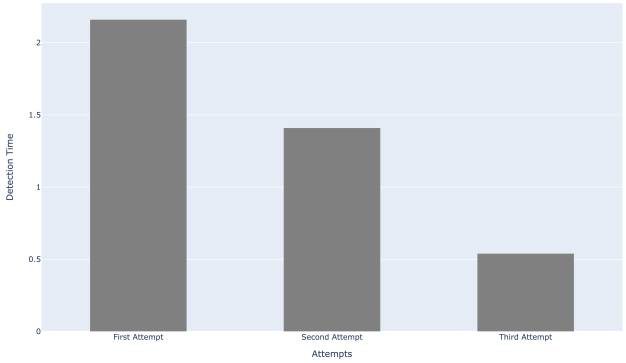


Figure 3: The time it took ActiveLock to detect the impostor after three attempts.

The observer impostor typed all 181 words after observing and learning the typing dynamics of the victim, and ActiveLock detected nothing. In the second and third observations, the attacker acquired more information and discovered that the victim's typing speed was quite quick and that the left thumb was used to press commands such as CAPSLOCK, SHIFT, and others.

Nonetheless, the attacker typed all 181 words with no detection from ActiveLock. Figure 4 shows the amount of time it took the attacker to type all 181 words.

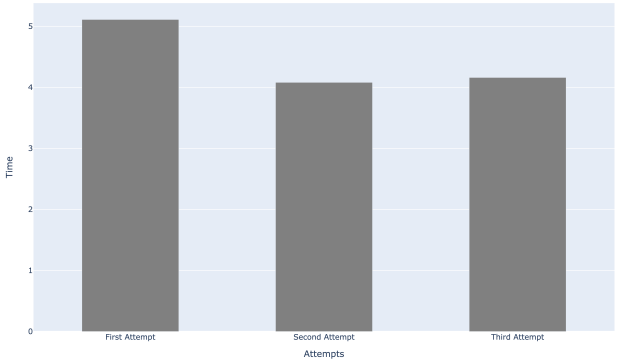


Figure 4: ActiveLock never detected the observer impostor in three attempts.

5.3 ActiveLock did not recognize any other forms of activity apart from typing

Another thing we made sure to evaluate was whether ActiveLock could detect both the impostor and observer impostor using the computer for anything other than typing. However, ActiveLock detected nothing. Despite the attacker visiting numerous websites and playing with the computer, ActiveLock failed to identify the imposters.

5.4 ActiveLock failed to detect the attacker when trying to log back into the computer

We attempted to determine whether ActiveLock could identify the impostors when signing back into the computer after the computer had logged the false users off, and we assumed the attacker already knew some login credentials. On the Mac, the attacker entered the password to log back into the computer, but ActiveLock did not detect anything.

6 LIMITATIONS

We faced a number of limitations while doing our research. First of all, we were unable to find any businesses willing to give us their demos or the chance to download and test out their free demos or SDK. Only businesses and not individuals were of primary interest to them. This presented a significant barrier for us because we really wanted to evaluate the effectiveness of other CA solutions as well as those that use different behavioural biometrics techniques.

Finally, there is a lack of substantial research on the evaluation of CA solutions; some studies on solutions utilising behaviour biometrics have been conducted, but none on *continuous solutions*, and for us, this was quite a disadvantage as we had no preceding work we could build on.

7 CONCLUSION

Although the technology behind continuous authentication appears to have great potential, more work still has to be done, particularly in relation to any CA solutions that may exist such as the one we evaluated in this research. Numerous aspects need to be figured out, such as what industry it should target in particular and the level of accuracy of the product.

The major goal of this study was to assess different CA solutions and use one as a case study (ActiveLock by TypingDNA), to determine whether the solution actually performs as promised. As the legitimate user did not encounter any false rejections and the impostor was rejected after three attempts, ActiveLock by TypingDNA performed quite well.

The app's greatest flaw, though, was that it never once rejected the observer impostor, raising significant security concerns. Also, the amount of time it took for ActiveLock to identify an impostor and log the impostor out was another major security risk because it took too much time subjectively. We believe that between the time the impostor took control of the computer and the time the app detected and logged the impostor out, a successful attack may have been executed.

Additionally, the app failed to recognise any other computer activity the impostor had engaged in, and it failed to recognise the impostor's typing biometrics when the impostor signed in again.

Future work will include, simulating an injury and testing whether the user experience of a legitimate user will be impacted, gaining access to other CA demos and evaluating them, working with various attackers and victims who have various typing patterns, and simulating a different type of attack, such as using a compromised biometric dataset to extract victims' typing patterns.

Based on our subjective views, we believe that combining mouse dynamics with typing biometrics would have made ActiveLock a much stronger product. In addition, we believe that ensuring quick impostor detection speed and fine-tuning the typing biometric accuracy behind ActiveLock, would result in a product that is much more resistant to imitation.

8 ACKNOWLEDGMENTS

Many thanks to Prof. Urs Hengartner for contributing some insightful and important information towards this research.

REFERENCES

[1] URL: https://www.typingdna.com/activelock-user-guide.
[2] URL: https://www.typingdna.com/behavioral-biometrics.html.
[3] URL: https://owasp.org/www-pdf-archive//Ksd.pdf.
[4] URL: https://www.typingdna.com/.
[5] URL: https://www.behaviosec.com/.
[6] URL: https://www.secureauth.com/.
[7] URL: https://zighra.com/.
[8] URL: https://nudatasecurity.com/.
[9] L.C.F. Araujo et al. "User authentication through typing biometrics features". In: *IEEE Transactions on Signal Processing* 53.2 (2005), pp. 851–855. DOI: 10.1109/TSP.2004.839903.
[10] Davrondzhon Gafurov, Einar Snekkenes, and Patrick Bours. "Spoof Attacks on Gait Authentication System". In: *IEEE Transactions on Information Forensics and Security* 2.3 (2007), pp. 491–502. DOI: 10.1109/TIFS.2007.902030.
[11] Yunji Liang et al. "Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective". In: *IEEE Internet of Things Journal* 7.9 (2020), pp. 9128–9143. DOI: 10.1109/JIOT.2020.3004077.
[12] Proximity Login Solution. *What is continuous authentication?* 2020. URL: https://gatekeeperhelp.zendesk.com/hc/en-us/articles/360056321214-What-is-continuous-authentication-.
[13] Biometric Solutions. *Keystroke Dynamics.* URL: https://www.biometric-solutions.com/keystroke-dynamics.html.
[14] Avi Turgeman. *Machine Learning And Behavioral Biometrics: A Match Made In Heaven.* 2018. URL: https://www.forbes.com/sites/forbestechcouncil/2018/01/18/machine-learning-and-behavioral-biometrics-a-match-made-in-heaven/?sh=7092b6fe3306.