Real-World Motion-Based Authentication

UNIFYID™

Introduction and Background

UnifyID is the first implicit authentication platform designed for use in the online and physical worlds. Our platform uses multiple passive factors to seamlessly authenticate individuals without requiring any conscious action by the user. One of the factors we use in authentication is an individual's gait signature, or how a person walks. **Gait signatures are a unique biometric signal that can be highly discriminative between individuals. Gait signatures can be obtained via motion sensor data from smartphones or wearable devices; it does not require any change to user behavior.** Combined with the possession of a physical device (a phone), a gait signature fulfills the need of multi-factor authentication as a unique biometric, without causing any additional friction to the user.

With data from millions of active users, UnifyID has detailed statistics on the real-world performance of gait signatures as a biometric factor. We establish gait signatures as an effective biometric and show how it can be as accurate as fingerprints or facial recognition in real-world scenarios, while also being less intrusive.

Learning a User's Model

The process of learning a user's model involves learning the shape and decision boundaries in a high-dimensional space to determine what makes each person's gait unique.

Using machine learning models that were trained with millions of users and billions of walk cycles, we found that features cluster tightly for a given individual and for a given mode of walking. In addition, the clusters are distinct between individuals. Figure 1 shows an example of clustering of different users walk cycles projected into three-dimensional space using the t-SNE visualization technique. The gait cycles tend to cluster tightly for individual users and are often completely dissimilar between users.

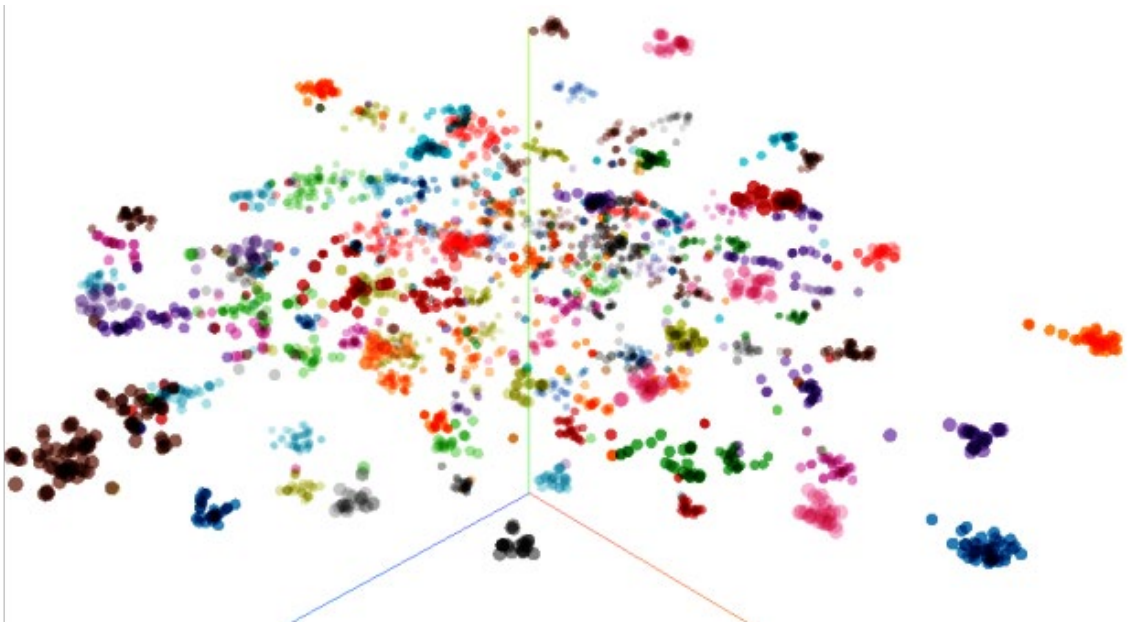

Figure 1: Clustering of gait cycles from 114 different users using t-SNE visualization, projected onto three dimensions

Classification Accuracy for Each Walk Cycle

Figure 2 shows the mean receiver operating characteristic (ROC) curve and accuracy rates for our entire test cohort on a per-walk-cycle basis. The ROC curve also includes a shaded region that represents the standard deviation of the ROC curves for the individual users. The mean AUC (area under the ROC curve) value, an aggregate value of performance, is 0.949. For comparison, an AUC of 1.0 means that the model's predictions are 100% correct.

The results show a very high level of accuracy even after a single gait cycle. **On average, our model rejects attacker walk cycles with a 96% probability.**

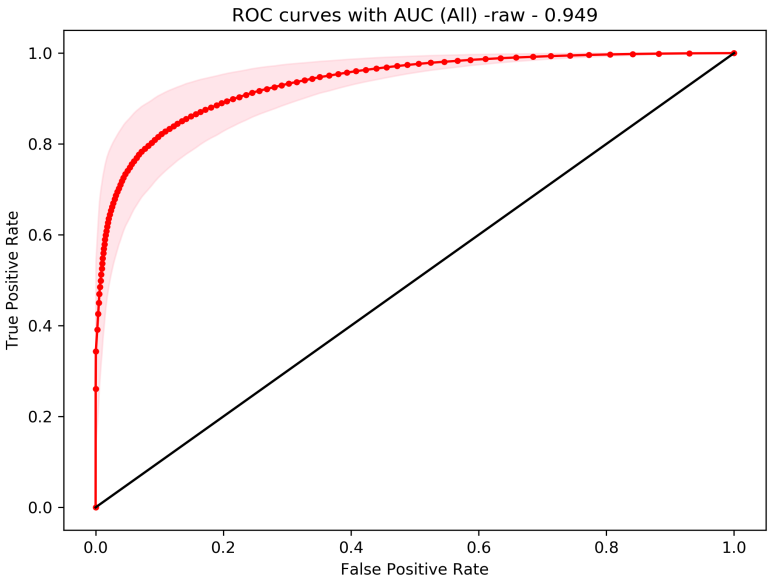

Figure 2: Mean ROC curve showing the overall accuracy on a per-gait-cycle basis across the entire test population. The shaded region shows the standard deviation around the mean.

Evolution of Gait Across Time

An individual's gait and behavior naturally shift over time (injury, age, pregnancy). To deal with these gradual changes, we employ perennial learning to track a user's natural behavioral changes over time. As new data is collected, the user model evolves, decaying older labeled data while weighing newer data more highly. Without perennial learning, a model trained on the earliest data performs poorly when tested with the most recent data. UnifyID's perennial learning system allows the model to be continuously updated while maintaining a high level of accuracy over time.

Defense Against Targeted Attacks

In this section, we evaluate the performance of UnifyID's gait-based authentication system with respect to classes of attacks, and discuss defenses against those attacks.

Mimicry

One possible attack against gait authentication systems is mimicry, whereby an attacker observes someone's gait and mimics it closely enough to fool the system. To evaluate the feasibility of such attacks, we recruited a group of volunteers, including some actors who are trained in identifying and mimicking behavioral mannerisms, to attempt to authenticate as another user. They were then allowed to observe the enrolled subject and attempt to mimic the subject's gait in an attempt to authenticate. In no case was the attacker able to authenticate as the legitimate user. This indicates that the features used in UnifyID's gait-based authentication are resilient to mimicry attacks.

Adversarial Attacks

Another class of attacks against machine learning systems is adversarial attacks, whereby a sophisticated attacker attempts to trick the machine learning system into a misclassification.

UnifyID has built protections against adversarial attacks on the machine learning component. We augment our training data to include attacks generated via known adversarial techniques as counterexamples, making the system robust to these types of attacks. Figure 3 shows the results of pre-training against adversarial attacks. The green line shows the probability of correctly classifying adversarial examples when adversarial training is performed, and the blue line shows the accuracy without adversarial training. The model performs significantly better with adversarial training.

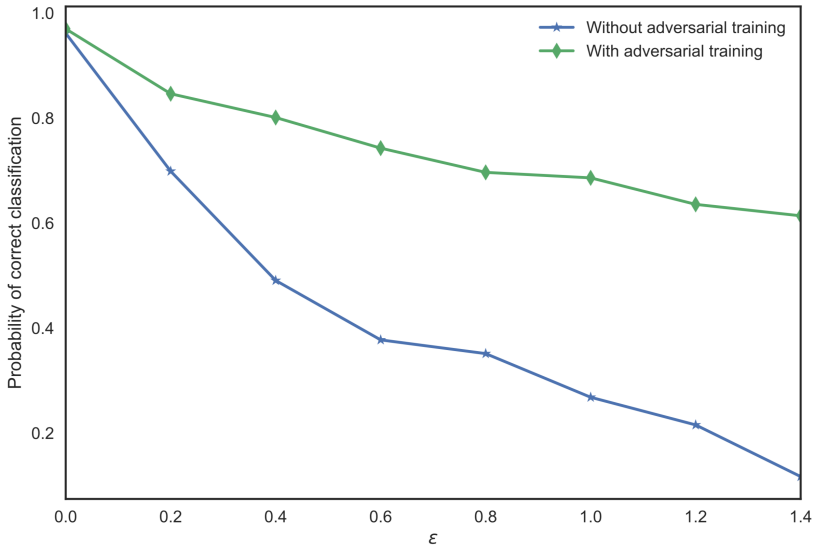

Figure 3: Comparing correct classification on adversarially-generated walk cycles when the system is pre-trained against adversaries (green line) and when there is no pre-training (blue line).

Summary and Conclusions

UnifyID's gait authentication is able to achieve high accuracy on a diverse set of users and scenarios. After one walk cycle, the solution achieves on average a 0.949 ROC-AUC and false positive rates of 4%. This means that our model has a prediction accuracy of 96%. As the number of walk cycles increases, the accuracy approaches that of state-of-the-art facial recognition systems, raising this prediction accuracy to 99%. This paper also covered possible attacks against gait-based authentication systems and showed how UnifyID's system is robust against those attacks.

UnifyID's highly sophisticated machine learning models enable the security of multifactor authentication without the friction associated with traditional methods. Our platform is based on the unique features of every individual, as are our values: the best way to authenticate yourself is to be yourself.