When Your Fitness Tracker Betrays You: Quantifying the Predictability of Biometric Features Across Contexts

Simon Eberz[1], Giulio Lovisotto[1], Andrea Patanè[1], Marta Kwiatkowska[1], Vincent Lenders[2], and Ivan Martinovic[1]

[1] *Department of Computer Science, University of Oxford, UK. Email: firstname.lastname@cs.ox.ac.uk*
[2] *armasuisse, Switzerland, vincent.lenders@armasuisse.ch*

Keywords: Biometrics, Authentication, Distributions transformation

1 Introduction

Attacks on behavioural biometrics have become increasingly popular. Most research has been focused on presenting a previously obtained feature vector to the biometric sensor. However, obtaining the victim's biometric information may not be easy, especially when the user's template on the authentication device is secured. As such, if the authentication device is inaccessible, the attacker may have to obtain data elsewhere. The key challenge lies in the fact that the distribution of biometric features strongly depends not just on the user, but also on the *context* of the measurement (e.g. different sensor or performed task). However, differences between contexts may be partly systematic, i.e., consistent and predictable for a large number of users.

In this work, we discuss an analytic framework that enables us to measure how easily features can be predicted based on data gathered in different contexts [1]. At the core of the framework lies a methodology for automatically deriving a cross-context feature mapping based on population data. This cross-context mapping works by optimising the intra-user statistical similarity between the feature values sampled from the source context and those sampled from the target context.

Using a dataset comprising of 30 participants and a variety of different contexts[1], we apply the framework to assess how resilient individual features and entire biometrics systems are against cross-context attacks.

2 Results

Briefly, we seek an optimal transformation of the random variable associated to the source context that minimise the intra-user statistical similarity with the corresponding random variable for the target context. The optimisation error of the optimal transformation thus measures how features from the source context can predict features from the target context.

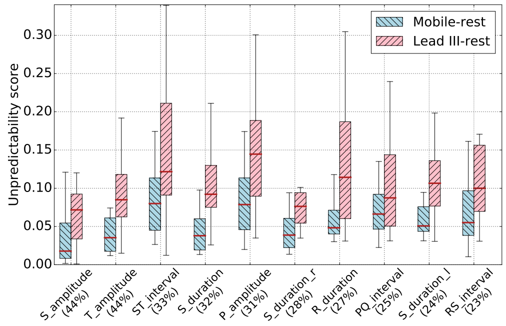

Figure 1: Unpredictability score of the most informative features for ECG. Features are sorted by relative mutual information (reported in percentage on the x-axis label).

We summarise here a few results obtained for ECG biometrics. In Figure 1 we compare *unpredictability score* for two source/target contexts for ECG biometrics (target: Nymi band[2], sources: *Mobile*[3] and *Lead III*). We can see how *Mobile* consistently outperforms *Lead III* for each feature. This can be explained by closer similarity of the ECG signal when measured at the extremity of the subject's arms (true for *Mobile* and the target *Authenticator*), compared to *Lead III* (measured at the extremity of left arm and leg). Similar results obtained using different sources highlight that ECG-based authentication might still be secure if the adversary steals ECG data from dissimilar contexts. However, since hand-based measurements are convenient and common, this highlights the danger of using the same type of measurement for authentication.

3 Conclusion

We have presented a framework that allows us to measure the unpredictability of biometric features across different contexts. The scores we compute provide fine-grained information about the resilience of biometric systems against cross-context attacks and can be used to: (i) compare biometric systems, (ii) identify vulnerable target contexts and for (iii) the selection and engineering of features.

References

[1] Simon Eberz, Giulio Lovisotto, Andrea Patane, Marta Kwiatkowska, Vincent Lenders, and Ivan Martinovic. When your fitness tracker betrays you: Quantifying the predictability of biometric features across contexts. In *IEEE Symposium on Security and Privacy*, 2018.

[1] Raw data available at `https://ora.ox.ac.uk/objects/uuid:0175c157-2c9b-47d0-aa77-febaf07fca71`

[2] `https://nymi.com/`

[3] `https://www.alivecor.com/`