April 7, 2025
Nomination statement for NSA Best Scientific Cybersecurity Paper Competition
(Nominator: Earlence Fernandes, UCSD)

Paper: Biosignal Authentication Considered Harmful Today
Authors:
Veena Krish, Stony Brook University
Nicola Paoletti, King's College London
Milad Kazemi, King's College London
Scott Smolka, Stony Brook University
Amir Rahmati, Stony Brook University

Recent advances in biosensing have sparked a growing interest in the use of physiological data for user authentication. Many commercially available wearables—such as smartwatches and fitness trackers—are now equipped with compact, affordable, and high-quality sensors that enable the collection of biometric data for cardiovascular health monitoring. The idea of repurposing these sensors for authentication has gained momentum for several reasons. First, many widely adopted authentication methods, such as passwords and fingerprints, suffer from well-documented vulnerabilities. Additionally, state-of-the-art machine learning techniques have shown impressive performance in extracting meaningful information from physiological time-series data. These developments have paved the way for "end-to-end" authentication systems that learn relevant features for user identity prediction along with training the system. Most critically, biosignals are generally assumed to be confidential— the prevailing assumption is that it is difficult for an attacker to observe or replicate someone's cardiovascular data.

In this work, the authors challenge this key assumption of confidentiality for biosignals and show that the uniquely identifying features found in a user's cardiovascular signal, such as the Electrocardiogram (EKG), can be consistently leaked from other types of cardiovascular signals from that user.
BioForge is a black-box spoofing attack on a variety of biosignal-based authentication systems, revealing that an adversary with access to alternative physiological information – such as pulse waveforms obtained through compromised devices, leaked datasets, or even video recordings – can generate spoofed signals capable of deceiving authentication models and masquerading as a target user. BioForge leverages a generative model to synthesize realistic physiological signals for a given user without relying on simultaneously collected training data. Their evaluation also demonstrates that multimodal authentication systems, which are often proposed as more secure alternatives, remain susceptible to spoofing when the included modalities involve different types of cardiovascular signals.

Looking ahead, risks in this domain will continue to escalate as generative modeling techniques advance, wearable devices become more prevalent, and the likelihood of data breaches increases. Overall, these findings underscore fundamental weaknesses in biosignal-based authentication systems and point to an urgent need for more rigorous security analysis in the design of future authentication technologies.