A Conversation with Tempestt Neal: Continuous authentication methods for mobile platforms

INNOVATION LEADERS

by Bushra Anjum

Editor's Introduction

Ubiquity's senior editor Dr. Bushra Anjum chats with Dr. Tempestt Neal to discuss her work to improve access control on mobile devices, specifically developing continuous authentication methods.

A Conversation with Tempestt Neal: Continuous authentication methods for mobile platforms

INNOVATION LEADERS

by Bushra Anjum

Dr. Tempestt Neal is an assistant professor at the University of South Florida's Department of Computer Science and Engineering. Her research focuses on mobile sensing technologies for human behavior analytics and biometric authentication. She is particularly interested in the fusion of sensor data generated in everyday environments such as homes and schools for activity and scene recognition to predict and detect physical and behavioral anomalies. She was the recipient of the NSF CyberCorps Fellowship and is a member of the ACM Future of the Academy. She is currently the IEEE Biometrics Council Women in Engineering liaison, an associate editor for the IEEE Biometrics Council Newsletter, and has served on several program and workshop committees. She earned her Ph.D. in computer engineering from the University of Florida. Dr. Neal can be reached via tjneal@usf.edu, Twitter: [@TempesttNeal](https://twitter.com/TempesttNeal).

Dr. Neal sat down with Dr. Bushra Anjum Ubiquity editor and ACM-W Standing Committees Chair, to discuss her work to improve access control on mobile devices, specifically developing continuous authentication methods.

What is your big concern about the future of computing to which you are dedicating yourself?

My research is in biometric authentication with a focus on continuous authentication. I care deeply about access control, educating people on access control mechanisms, and creating methods to automate access control. I've particularly focused my efforts on user authentication for mobile devices; today's devices have become extremely integrated into our everyday lives, especially since they allow people to store and manipulate data on the go. Consequently, access control is severely important, and many devices provide users with password or biometric-based authenticators. There are two key concerns, however, that reduce the efficacy of both methods. First, either input is only requested at the point-of-entry (PoE); the lack of continuous authentication places the user's session at risk of hijacking. Second, research shows that many individuals do not employ an authentication method at all on their device, and a portion of those that do choose easily guessed passwords such as "123456," reducing the need to remember and frequently re-enter complex combinations of characters. Although biometric identifiers are not associated with increased memory load, current commercial implementations of biometrics do not address the first concern. These two problems are

difficult to resolve due to variations in devices (consider the IoT ecosystem), considerations in data privacy (not all biometric data is suitable for every domain), and the heterogeneity of streaming biometric data (data fusion in real-time). By researching these problems, I hope to improve access control by developing new continuous authentication methods suitable for mobile platforms.

How did you become interested in the field of access control, specifically biometric based identification?

My research stemmed from my advisor's research, which spanned biometric identification, computer vision, and pattern recognition. I had no intentions of pursuing a Ph.D. when first entering college; I was very unfamiliar with research and graduate school until I actually pursued it. It was rare to hear stories of people going to graduate school and even rarer to hear of anyone finishing while I was in high school. I was sure that I would work toward a bachelor's degree and did so successfully with very little exposure to research. I was exposed to one biometric system while working as an intern; the company¹ required employees to register their handprint as a part of onboarding. Even then, it was a new yet uninspiring experience.

While approaching the end of my undergraduate studies, I started pondering what I wanted my career to look like. At the time, the last three to four years were largely immersed in learning to program; naturally, I decided to continue my education as a master's student to eventually start a career as a software engineer. However, even before receiving one acceptance letter to a M.S. program, an opportunity fell into my lap that I didn't realize would completely lead to a new path—one more exciting and certainly more filled with ups and downs.

I was invited to attend a two-day in-person meet-and-greet at Clemson University during which seniors from HBCUs [historically Black colleges and universities] were introduced to various faculty, their graduate students, and the research within their labs. I was fascinated by the culture that Clemson had built, especially around African-American and female students. There was an eclectic mix of research goals (none that I had ever considered) that felt, at least, achievable. Interestingly, my would-be graduate advisor was a part of the mix, even though I didn't actually get to meet with him during that weekend. However, I was approached by Dr. Juan Gilbert, the chair of one of the CS departments at the time; he connected Dr. Damon Woodard, my would-be advisor, and me through email shortly after the visit. As cliché as it sounds, the rest is history. His mentorship and willingness to take on a lost but motivated student was critical to my pivot toward the pursuit of a Ph.D. (although I'll admit to entering the program to primarily "see how it goes").

As time went on and I grew more knowledgeable of biometric research, not only did my desire to complete the degree grow, but I also grew passionate about the task of access control in a

¹ The company's name is not disclosed to protect any confidential information.

broader sense (not just through biometric identifiers). For instance, studies show that many choose easily guessed passwords for controlling access to data stored on their personal devices; I want to know more about these occurrences and how passive biometrics can help automate access control to reduce the use of poorly chosen passwords. Studies also show that some people prefer the use of passwords over biometrics due to privacy concerns; I want to know more about how to change the narratives of access control mechanisms like passwords and biometrics to increase the public's trust.

What projects are you leading that are focused on behavior based continuous authentication? Would you like to share some interesting findings from your work so far?

Commercial mobile devices currently employ PoE (e.g., passwords/PINs, face/fingerprint recognition) authentication methods for controlling who accesses a device. Several studies show that knowledge-based authenticators like passwords are ineffective; strong passwords are difficult to remember and it can be a pain to frequently request admin services to reset them. PoE and knowledge-based authenticators are both ineffective throughout sessions of use; once a person is authenticated; the device and its content remain available to the current user (whoever that may be). My current research explores various data-based usage patterns of a mobile device as behavioral biometric modalities, including patterns in application use, networking activity (i.e., Bluetooth and Wi-Fi sightings), and communication through calling and text messaging, which can continuously and passively authenticate a device's owner. Thus far, we've demonstrated the use of association rules for learning distinct usage patterns in user-device interactions, including patterns in how a person uses their mobile apps. We've also shown how association can be useful for data fusion, which proved significant in improving user recognition performance. We've explored the effect of gender on user recognition performance as well, finding that gender may play an important role in verifying who is using a mobile device. For example, we found higher activity levels from female subjects compared to male users in mobile app use and were able to find differences between them based on transitions from and to sports, navigation, and system-related apps and number of revisitations to apps within sessions [1]. We've also developed and studied the detection of attack scenarios in which a mobile device may have been stolen (and thus the current user is not authorized to access the device). Our experiments showed that our attack models can lead to an attacker being falsely verified as an authorized user with up to a 50 percent success rate, demonstrating a significant open challenge in this domain. Although we have continued to explore continuous and mobile biometrics by branching into some physical biometrics (e.g., face) and new feature representations (e.g., behavior profiles), there are several areas of interest that I hope to pursue over the next few years (e.g., continuous authentication on IoT devices).

Reference

[1] T. Neal and D. L. Woodard. A gender-specific behavioral analysis of mobile device usage data, 2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA), Singapore, 2018, pp. 1-8. doi: 10.1109/ISBA.2018.8311459

Biography

Bushra Anjum is a software technical lead at Amazon in San Luis Obispo, CA. She has expertise in Agile Software Development for large scale distributed services with special emphasis on scalability and fault tolerance. Originally a Fulbright scholar from Pakistan, Dr. Anjum has international teaching and mentoring experience and has served in academia for over five years before joining the industry. In 2016, she has been selected as an inaugural member of the [ACM Future of Computing Academy](#), a new initiative created by ACM to support and foster the next generation of computing professionals. Dr. Anjum is a keen enthusiast of promoting diversity in the STEM fields and is a mentor and a regular speaker for such. She received her Ph.D. in computer science at the North Carolina State University (NCSU) in 2012 for her doctoral thesis on Bandwidth Allocation under End-to-End Percentile Delay Bounds. She can be found on Twitter [@DrBushraAnjum](#).

DOI: 10.1145/3404394