Predicting Authentication Performance with Psychological Constructs

Seth Hastings with
Dr. Tyler Moore, Dr. Sal Aurigemma, Dr. Bradley Brummel
University of Tulsa
Seth-Hastings@utusla.edu

Abstract

This study examines the relationship between end user's scores on psychological constructs and observed performance and usage metrics derived from Azure AD sign-in logs under a variety of Multi-Factor Authentication (MFA) configurations. Five security relevant psychological constructs were assessed through a survey measure in a study population of 162 students and faculty at the University of Tulsa, Oklahoma. A system of encoding sign-in logs was created to provide single-line reporting of an individual experience by a user, which we call an "event", reducing 721,493 raw log entries to 36,658 user interactive "events". Analysis of correlations between usage patterns and psychological constructs is ongoing.

Purpose

This study seeks to deepen understanding of end user's authentication performance which could enable informed, targeted interventions to improve user experience. Modern identity and authentication management systems provide many sources of data on user behavior and can be configured in numerous ways. With the increasing adoption of multi-factor authentication (MFA), this study seeks to examine the differences in use patterns and performance for users with various types of MFA sources under a variety of configurations. While some work has been done to understand security related psychological constructs and how these individual differences shape user interactions, this work has been primarily based on self-reported computer performance from users. This paper compares user's scores on security focused constructs with observed network behavior and performance over time. This enables us to examine connections between different types of MFA and user performance while incorporating the user's individual psychology. Gaining insight into these patterns could inform interventions for targeted improvements to a user's experience. This study predicts these usage patterns using five security relevant psychological constructs. Constructs measuring security related Overload, Complexity, and Uncertainty were adapted from D'Arcy et al. (2014), General Self-Efficacy (GSE) and Security Related Self-Efficacy (SRSE) from Chen et al. (2001) and Compeau et al. (1995) respectively. The survey instrument used captures these constructs and open answer qualitative responses on user attitudes towards mandatory MFA and other TU security policies.

Design/Methodology

We used two primary measurement tools across a single group consisting of students and faculty at the University of Tulsa. Between October 12, 2020, and January 18, 2020, 167 participants completed a survey to gather construct scores and additional qualitative responses around security policy and implementation at TU. 162 respondents chose to participate in the study. The second tool is constructed from user sign-in logs produced in the Azure AD system spanning the year 2022. A system of encoding and aggregating these sign-in logs was created to provide single line reporting of an individual experience by a user we call an "event", representing a user attempting to sign on to a specific application. This includes the number of errors encountered before eventual success or failure, as well as the type of errors involved, time spent on an attempted authentication, and the type of authentication used. The study population is viewed through the lens of these events, and reveal connections between various usage patterns and outcomes, and between MFA types and outcomes. We examined 721,493 raw log entries

which reduced to 36,658 authentication events. The data collection and encoding processes is shown in Figure 1.

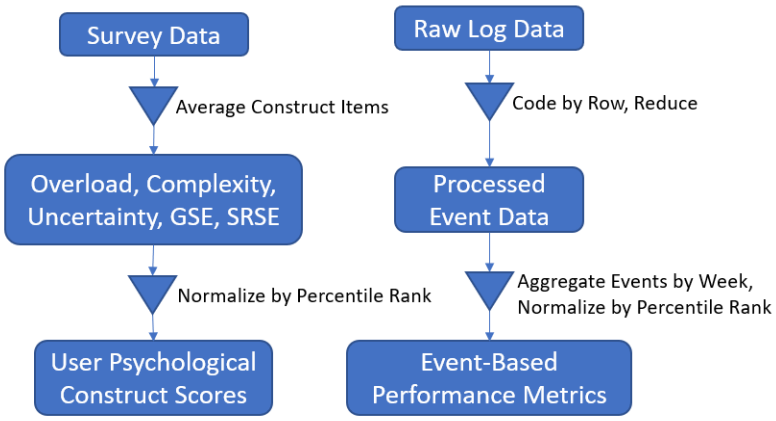

Figure 1 – Data Processing Flow Diagram

Findings

Data collection and analyses are ongoing with plans for further onboarding. Initial results show bias towards "better" forms of MFA prompts such as App Notification, with 60% of users utilizing, compared to 10% utilizing Phone Call based MFA, as well as higher performance for the users utilizing the "better" MFA. The "event" view represents the primary database for analysis and has spawned multiple derivative datasets with variables focused on quantifying performance across settings and users. Simple correlation between several performance metrics and the measured security constructs are seen in Table 1. The performance metrics are normally distributed and based on the user's percentile rank in the study population. Variable 6 captures a user's average time spent on a successful authentication, 7, the user's ratio of total time spent on successful authentications to total time spent on failed authentications, which is tracked in seconds. Variable 8 captures the number of successes per minute spent authenticating. Initial testing shows strong test-retest reliability of derived usage and performance metrics, although more work needs to be done to confirm these results. While performance metrics are not highly correlated with constructs in this analysis, investigation into rarer performance items is ongoing, and more complex analysis is required to constrain analysis to groupings of users with similar performance.

Table 1 - Construct Correlations

	1	2	3	4	5	6	7	8
1. Security-Related Complexity	-							
2. Security-Related Overload	.16	-						
3. Security-Related Uncertainty	-.73***	.06	-					
4. New General Self Efficacy	-.07	-.04	.09	-				
5. Security Related Self Efficacy	-.07	-.01	0.04	.56***	-			
6. Time Per Successful Authentication	.06	-.08	-0.1	.19*	.39***	-		
7. Ratio of Time Succeeding to Time Failing	-.01	.02	0.01	-.08	-.04	-.03	-	
8. Success Per Minute Spent Authenticating	.08	-.19*	-0.2	-.25**	-.26**	-.11	.06	-

* p < 0.05; ** p < 0.01; *** p < 0.005.

Research Limitations/Implications

The primary limitation is small study size, wtih many initial participants no longer interacting due to graduation. Second, many of our study participants come from the same departments at TU; diversification of the study population would benefit the validity of our results. The "event" view developed for the analysis may improve the performance of SOC's by enabling SOC's to quickly assess the state of a user's authentication and note changes in usage and performance patterns through a simplified view. Second, the relative performance difference between types of MFA prompt used implies the opportunity to improve user performance through configuration changes that shift users to more efficient ways of authenticating. Third, the event view of sign in data clarifies population and individual user pain points (Configuration issues, User Errors, and Hacking Activity).

Originality/Value

The Overload, Complexity, and Uncertainty constructs are relatively new (circa 2014). To our knowledge, this study is the first to combine these constructs with observed user behavior as an objective measure. The ability to compare various psychological constructs generated from participants self-report data to that same user's actual behavior on a network affords a unique opportunity to draw connections between psychology and performance in a way not yet seen in the literature. This methodology offers the opportunity for multiple assessments to validate future interventions based on a user's performance.

References

1. D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. Journal of Management Information Systems, 31, 285-318. doi: 10.2753/MIS0742-1222310210
2. Chen, G., Gully, S. M., Eden, D. (2001). Validation of a new general self-efficacy scale. *Organizational Research Methods, 4,* 62-83. https://doi.org/10.1177/109442810141004
3. Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. MIS Quarterly, 19, 189-211. doi: 10.2307/249688