TAG CYBER

ADDRESSING THE MODERN ENTERPRISE AUTHENTICATION CHALLENGE

EDWARD AMOROSO, TAG CYBER

VERIDIUM
TRUSTED DIGITAL IDENTITY

ADDRESSING THE MODERN ENTERPRISE AUTHENTICATION CHALLENGE

EDWARD AMOROSO, TAG CYBER

Despite universal agreement that strong authentication is a requirement, many enterprise teams continue to demonstrate slow deployment. In this article, we review the forces influencing modern authentication and recommend means for improving adoption and use.

INTRODUCTION

Modern authentication has progressed considerably from early reliance on password selection to more advanced technologies such as multifactor authentication and passwordless security. This is good news for anyone concerned with cyber risk, because the process of validating identity, whether for humans or devices, remains one of the most powerful means for stopping a determined adversary.

Despite such clear recognition of the importance of strong authentication, many enterprise teams continue to struggle with deployment and support. Our work at TAG Cyber regularly involves security advisory to major corporations and government agencies – and it is not uncommon for our analysts to encounter teams that continue to rely on passwords (or even IP source authentication) as a primary control.

In this article, we outline three forces that affect and influence authentication – namely, security, usability, and accessibility. We show how these forces can create friction between designers of digital experience and security engineers, and we offer some suggestions for how deployment of stronger forms of authentication might be best integrated into modern business and commerce applications.

FORCES INFLUENCING AUTHENTICATION

The business forces that drive decisions about authentication come down to three primary considerations, each of which requires attention from the designers and purveyors of digital experiences:

- **Force 1: Security** – It is obvious to any observer or participant in modern digital applications that threats have increased beyond any reasonable threshold. The FBI reported, for example, that they received nearly a million complaints of cybercrime in 2021 resulting in almost seven billion dollars in losses. [1]
- **Force 2: Usability** – It should also be obvious to any observer that the success of digital experiences, including eCommerce applications, is often determined by ease-of-use considerations. Customers who have trouble gaining access to a service, perhaps due to a forgotten password, will often just move to another service.
- **Force 3: Accessibility** – The final force affecting and influencing authentication is the overall accessibility of the control. This refers to the usability and simplicity associated with the password, cryptographic certificate, token, or other means being used to establish and prove a reported identity.

Each of these forces have an impact on the friction that is introduced to the user or customer experience. Security engineers view friction as a necessary attribute to counter threats, but digital experience managers, eCommerce operators, and IT service designers see friction as being something that must be minimized under any set of circumstances.

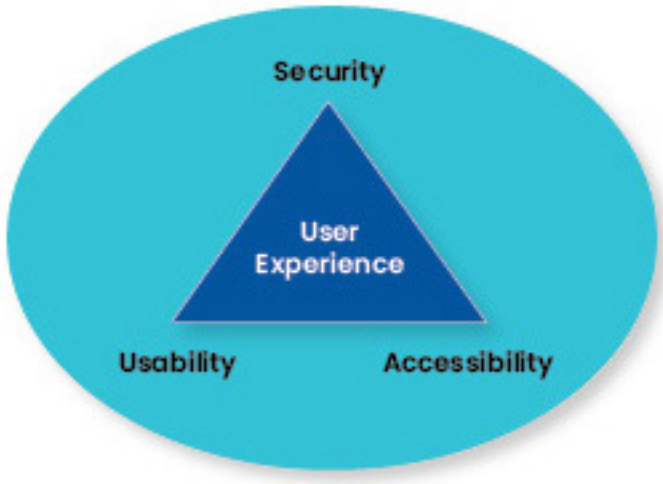

Figure 1. Forces Affecting Authentication Friction

[1] *www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf*

ADOPTION RECOMMENDATIONS

To optimize the adoption of stronger forms of authentication, we recommend that three approaches be used – each of which is designed to reduce the overall friction associated with whatever strong validation controls are selected. These recommendations, which are briefly outlined below, are based on many years of experience trying to balance the needs of security engineers and experience designers.

- **Recommendation 1: Early Design Cooperation** – Too often, the security engineering team will make its decisions about a selected authentication means without input or participation from other team members. It is highly recommended that the review, assessment, test, and analysis of authentication tools be an inclusive task. The result will be much higher adoption rates for the solution ultimately selected.
- **Recommendation 2: Flexible Solutions** – The decision to select a flexible solution involves assurance that the authentication control can be adjusted, tailored, and modified based on reported experiences. This also will go a long way to reducing friction between security and experience designers, because any issues reported by users can prompt adjustments in the experience.
- **Recommendation 3: Reliance on Metrics** – This is an important consideration, one often ignored in practical deployments. Accurate metrics from live production deployment should guide decision-making about authentication. It should never be the case that business leaders make decisions based on anecdotal views, but rather all decisions should be guided by data collected from actual users.

Each of these recommendations should serve to optimize the balance between security teams members who must deal with threats and business leaders who must ensure that their systems are easily accessible by users and that on-line systems and services provide a great experience for customers.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

Copyright © 2022 TAG Cyber LLC. This report may not be reproduced, distributed, or shared without TAG Cyber's written permission. The material in this report is comprised of the opinions of the TAG Cyber analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy, or completeness of this report are disclaimed herein.