THE TREND TOWARD DECOUPLED, INTEROPERABLE AUTHENTICATION AND IDENTITY

Authored by: Dr. Edward G. Amoroso, TAG Cyber

Originally tightly bound into systems, identity and authentication have gradually decoupled to support initiatives such as passwordless security. A new model called INZ has emerged in which identity, authentication, and authorization objectives are decoupled and supported through modular design.

Introduction

In our cybersecurity research at TAG Cyber, we've begun to rely on an emerging model of the interactions and interdependencies between identity, authentication, and authorization. This triad of related controls helps to frame how enterprise security programs should balance user experience, cyber risk mitigation, and support for network and computing architectures that are moving increasingly to cloud services.We refer to this triad model as INZ (Identity, Authentication, and Authorization).[1] A major aspect of the model is that the component functions should be modular, simple, and accessible through open interfaces. In a sense, the respective security functions should be decoupled in their design so as to enable more flexible interoperability and integration into existing and planned deployments.

The recent executive order on cybersecurity[2] from the Biden administration underscores the importance of this emphasis on getting the balance correct between these identity-related concepts. The order specifically references the zero-trust architecture model, in which identity plays a central role in securing applications and systems in a modern distributed multicloud hosting environment.

In this article, we focus on the decoupling of identity and authentication, with a focus on defining the specific interfaces that must be present to enable their integration in a live environment. We begin with an overview of present authentication methodsand then show the identity-related functions that must be accessible through modular interfaces for proper INZ model operation to proceed.

Evolution of Authentication

Authentication was originally designed as a fully integrated aspect of the computing experience for users. You accessed a system, and it included a login procedure that was part of the functionality. This process almost always included a password, and as any observer will attest, this has led to nothing but trouble in cyber security ever since. Passwords are easy to guess, difficult to secure, and inconvenient to maintain.

The first fix to this problem involved the introduction of two-factor authentication (2FA). This beganwith handheld authenticators, and quickly moved to include other types of complementary factors. Biometrics became important, especially with Apple integrating touch and facial recognition into its devices, and the mobile became essential for any type of out-of-band text push to enable authentication.

Today, the trend has arrived at full use of multi-factor authentication (MFA), with three primary goals: First, the authentication process is being simplified to maximize compatibility with cloud andother access scenarios (as referenced in the Biden executive order); second, the process is being strengthened to deal with the ever-expanding threat from adversaries; and third, the process is being streamlined to reduce friction for users trying to access new types of services.

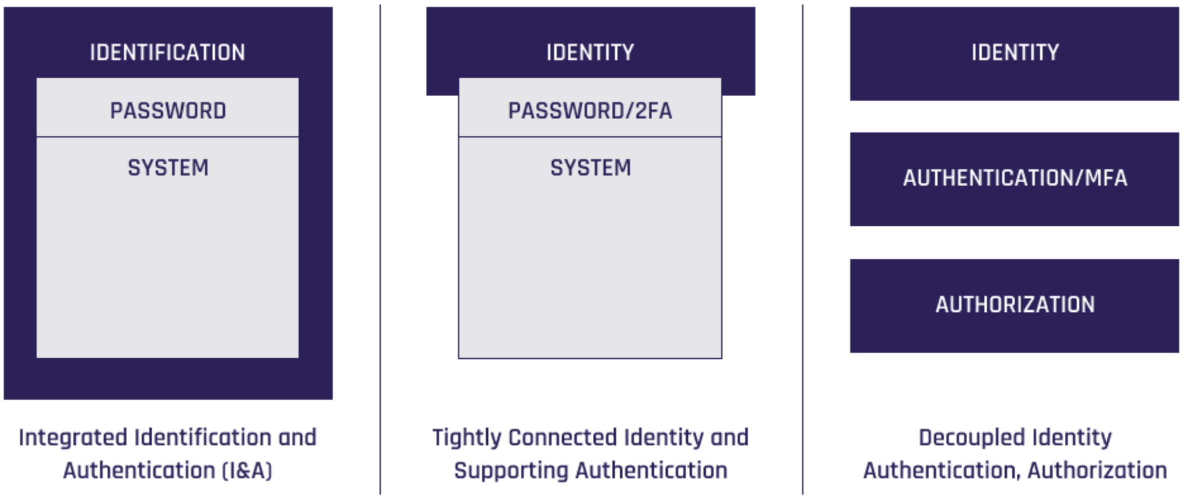
IDENTIFICATION
PASSWORD
SYSTEM
Integrated Identification and Authentication (I&A)
IDENTITY
PASSWORD/2FA
SYSTEM
Tightly Connected Identity and Supporting Authentication
IDENTITY
AUTHENTICATION/MFA
AUTHORIZATION
Decoupled Identity Authentication, Authorization

Figure 1. Evolution of Authentication

A major advance in authentication today involves the extension of MFA toward a fully passwordless experience. In such an arrangement, no stored passwords exist as a target for attackers, thus resulting in significantly reduced cyber threats. The improved cost implications for the typical enterprise are also significant, since password reset costs, which can be considerable, are also deeply reduced.

To summarize, the evolution of authentication can be viewed as a stepwise decoupling of the various components. Early system-embedded identification modules were replaced with identity providers (IdPs), which helped to drive greater focus on the need to validate the actual identity of individuals, systems, and other entities. More recently, authorization has emerged as an additional supporting activity.

Decoupling Model (INZ)

The most important aspect of this decoupling process has been the emergence of clearly defined separate interfaces between authentication functions and identity-related tasks such as proofing. Ultimately, the goal is to balance the need for a good user experience, low maintenance costs for operators, and sufficient multi-factor security to support protection and compliance requirements. The benefit of decoupling is that it gives options to organizations providing services to end users. The most attractive option is that a security team might choose to avoid traditional identity platforms that can be complex and dependent on passwords in favor of a passwordless platform that specifically prohibits use of passwords. Such a transition is only possible if the underlying mechanisms are no longer tangled together in an implementation.

This emphasis on interoperability, modularity, and decoupled design also extends to authorization, which complements the identity and authentication functions. The decoupling process also allows an enterprise to deal more effectively with cloud services such as Microsoft Azure, Amazon Web Services,and Google Cloud Platform, which have essentially moved into the identity business, supporting billionsof user identities.

To help visualize the end goal, a simple model is proposed where identity (I), authentication (N), and authorization (Z) are included. Interactions between these respective capabilities are central to the model and defined to support digital transformation, avoid the MFA fatigue that comes with multiple security authentication apps, and address references to standards such as FIDO in publications such as NIST SP 1800-17.

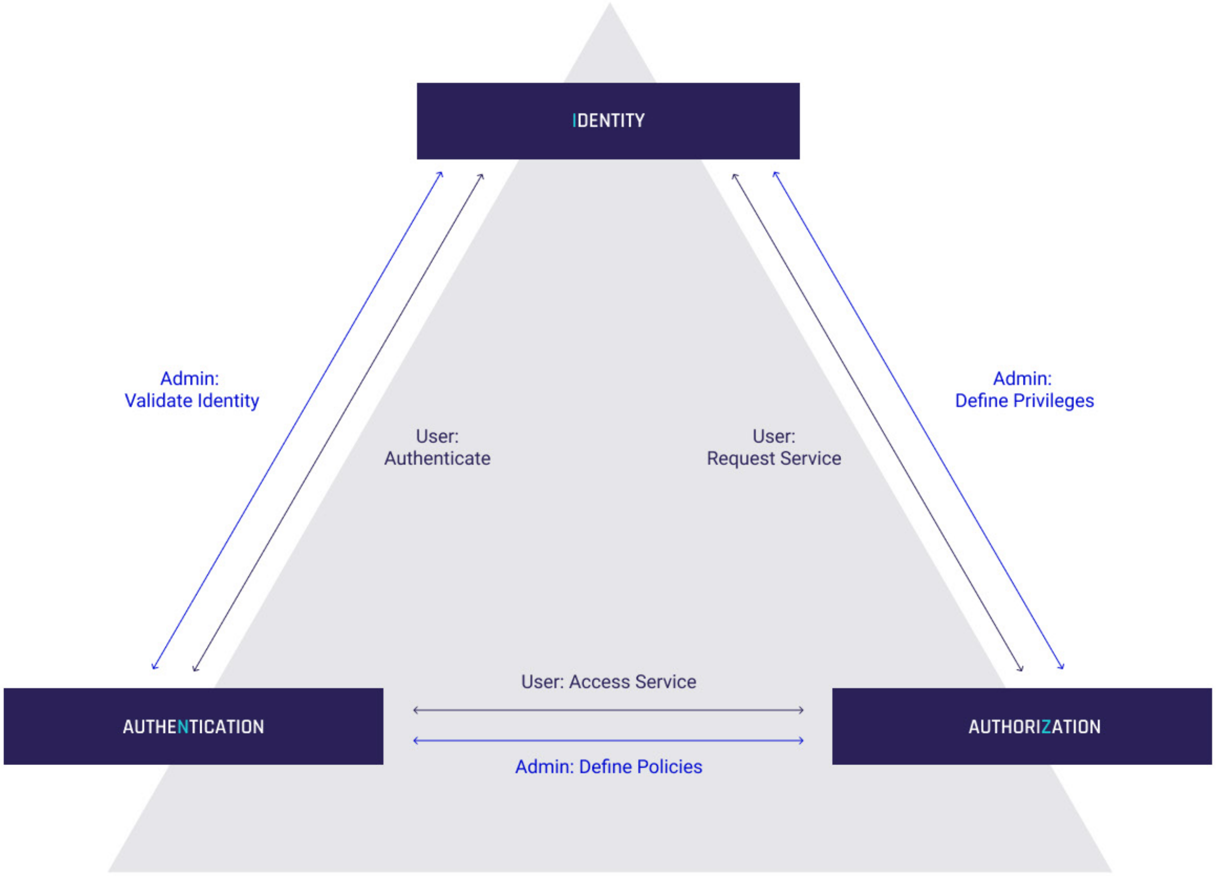

Figure 2. INZ Model

The INZ model highlights the need to define interactions between the components. That is, identity andauthorization have interdependencies that must be clearly defined. This is also true for authorization and authentication, and for authorization and identity. Advanced commercial platforms might cover many of these interfaces at once, but organizations must nevertheless ensure coverage in theirimplementation.

TAG Cyber research on the implications of using INZ continues with investigation into the interactions necessary between identity, authentication, and authorization — and underlying security architecture controls based on secure access service edge (SASE) enterprise designs. Cloud services, in particular,must work well with new passwordless authentication. Readers should expect additional research to become available throughout 2021.

Action Plan

Organizations providing services to users are advised to put together an INZ-based road map toward a modern, passwordless experience where identity, authentication, and authorization are fundamentally decoupled. The action plan associated with such a road map will likely include the following management steps, many of which might be well underway in the enterprise:

1 Take Inventory of All Identity, Authentication, and Authorization Processes

This step will be more involved for larger organizations that provide a wide range of services to users, employees, suppliers, customers, and other individuals and groups. It is nevertheless necessary to understand the organizational profile for these important functions. Particular focus should be placed on whether identity providers might prevent a transition to passwordless experiences.

2 Commit to a Common Passwordless Experience

The primary advantages of removing passwords should be clear: By avoiding the use of a storedpassword repository, organizations dramatically reduce their risk or breach, while also significantlyreducing the friction that comes with the need for users to remember and support multiple methods for identification, authentication, and even authorization. Commercial vendors supporting passwordless security are available, so this goal is feasible to achieve.

3 Communicate Modular Requirements to Supporting Vendors

Organizations are urged to engage in a healthy dialogue around identity, authentication, and authorization with their vendors. The INZ model might serve as a useful discussion guide — one that can be used to position a commercial vendor in the overall ecosystem. In the end, organizations must select and work with vendors who share the common goal of optimizing both security and the user experience.

[1] TAG Cyber has published its research on the INZ model in the Third Quarter TAG Cyber Security Report (see https://www.tag-cyber.com/advisory/quarterly/request?download=b0666e4a-799e-4604-9db9-27618d68728e&pub=TAG%20Cyber%20Security%20Quarterly%202021%3A%20Quarter%203).

[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

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.

THE PASSWORDLESS COMPANY

Contact: 1-866-GET-HYPR [US]

Learn more: www.hypr.com

HYPR reimagines multi-factor authentication to protect workforce and customer identities at the highest level of assurance. With HYPR True Passwordless™ MFA, you can change the economics of attack, improve your security posture, and enhance digital engagement with every login experience.