TAG

ADDRESSING API SECURITY REQUIREMENTS IN THE CONTEXT OF AUTHORIZATION AND POLICY-BASED ACCESS CONTROLS

DR. EDWARD AMOROSO,
CHIEF EXECUTIVE OFFICER, TAG

plainID
THE AUTHORIZATION COMPANY

TAG

ADDRESSING API SECURITY REQUIREMENTS IN THE CONTEXT OF AUTHORIZATION AND POLICY-BASED ACCESS CONTROLS

DR. EDWARD AMOROSO, CHIEF EXECUTIVE OFFICER, TAG

This TAG report provides an overview of API security requirements in the context of enterprise authorization and policy-based access controls (PBAC). Commercial vendor PlainID is shown to effectively implement authorization and PBAC for API security.

INTRODUCTION

Early generation computing involved mostly human beings interacting with digital systems – and the *human-machine interface (HMI)* that emerged was the subject of consideration time and attention for early security experts. Even today, security issues emerge as humans are exposed to phishing attacks on their computer screens, and research continues around how best to reduce this nagging risk.

More modern computing now relies increasingly on software interacting with its environment through so-called *application programming interfaces (APIs)*, which is how software systems such as applications and workloads communicate and share data. As one might expect, the corresponding security issues for APIs can be challenging, and enterprise teams are wise to seek capable commercial vendor partners to address the risk.

In this note, we explain how API security demands complementary focus on two additional aspects of modern cybersecurity – namely, *authorization* and *policy-based access control (PBAC)*. Both of these security controls are essential for good enterprise protection, but neither has been traditionally viewed as elements of the API security suite. We explain here why this has since changed and what this means for security teams.

AUTHORIZATION AND PBAC

It’s helpful first to explain what we mean by authorization and PBAC, since both concepts have tended to be under-attended by security teams. Authorization involves ensuring that the right individuals or systems have access to specific resources and functionalities while denying access to unauthorized entities. For APIs, this process is made more difficult by the diversity of users and the granular control required for API access.

The complementary method known as Policy-Based Access Controls (PBAC) has evolved as a practical approach to addressing the complexities of authorization and access control. PBAC leverages well-defined policies to determine access rights, thus providing a structured framework for API authorization. Experience has shown, however, that implementing PBAC within an API ecosystem can be non-trivial.

To illustrate, consider that a fundamental aspect of API security involves distinguishing between authentication and authorization. Authentication, as practitioners know, involves validation of a reported identity from some user or system. Authorization, on the other hand, defines what actions the authenticated entity is allowed to perform. Addressing the interplay between these two facets of cybersecurity is where authorization and PBAC can be useful.

ENTERPRISE API SECURITY REQUIREMENTS

For most developers, the connection between API security and authentication involves the use of so-called *API keys* – and developers will be the first to share their frustration regarding the challenge of managing API keys, especially for large development projects. The most common problems involve administering key rotation, key revocation, and ensuring that keys are not inadvertently exposed. None of these tasks lend well to manual effort.

Where authorization challenges emerge is when users and systems require access to APIs. This is done in the context of authorization policies that rely on API keys and other controls to implement proper access rights. Enterprises deal with vast numbers of users and systems that require API access. Ensuring that authorization policies scale efficiently while maintaining performance is a formidable challenge.

Slow or inefficient authorization processes can hinder operational agility. Furthermore, effective API security demands granular control over access rights. Enterprises may need to define policies governing different aspects of API access. This complexity can lead to challenges in policy management and enforcement. Real-time decision-making regarding API access is thus essential.

Traditional access control mechanisms struggle to keep pace with the dynamic nature of API interactions. Real-time policy evaluation and enforcement are prerequisites for effective API security. In addition, comprehensive logging and auditing are crucial for API security. Enterprises require detailed records of API interactions for security and compliance, and this necessitates logging mechanisms to capture relevant data without impacting performance.

ZERO TRUST, CONTEXT, AND INTEGRATIONS

The concept of Zero Trust, invented at Forrester several years ago, advocates for the continual verification of entities and devices attempting to access resources. The model gained prominence across the enterprise security community as perimeters became less effective at protecting hybrid networks. Implementing Zero Trust principles within the context of API security requires the integration of authentication and authorization controls.

To enact granular authorization and PBAC, enterprises must be aware of not only the identity of the entity seeking access but also the context in which the access request is being made. This includes factors such as the user's role, location, time of access, and the device being used. Integrating these various contextual elements into the authorization process is a non-trivial task for enterprise teams, especially if APIs are involved.

Enterprises must also contend with an ever-evolving external threat landscape. Malicious actors continually probe for vulnerabilities within APIs to gain unauthorized access. This necessitates continuous monitoring, threat detection, and proactive measures to safeguard APIs from external threats. An entire industry has emerged specifically to address API security weaknesses in the context of hybrid cloud deployment.

Finally, enterprises rely on third-party APIs to extend the functionality of their applications. Integrating external APIs introduces a layer of complexity in ensuring that third-party access aligns with internal authorization policies. This is a key consideration in practice, as most CISOs would view the risk associated with third parties as being perhaps the most challenging aspect of their overall cyber risk management program.

API REQUIREMENTS FOR SECURITY

As TAG analysts, we believe that API security in the context of effective authorization security and PBAC involves a tough balancing act. On the one hand, enterprises must enforce strict controls to mitigate the risk of unauthorized access and data breaches. On the other hand, however, overly restrictive access controls can impede productivity and hinder the seamless flow of data and functionality within the organization.

Accordingly, we recommend that modern enterprise security teams grappling with API security in the context of their authorization and PBAC implementation requirements focus their planning, design, and deployment attention in the following areas:

1. *Comprehensive Policy Framework*: Enterprise teams should first develop a well-defined and comprehensive policy framework that encompasses all facets of API access. This should link to the organizational mission and should consider the threats targeting the resources offered behind the API layer.
2. *Contextual Awareness*: Identity and context awareness are essential focus areas to enable granular control over API access. A problem with modern access controls is that the level of granularity for rights and permissions is usually insufficient – and with the added need to support authorization, including delegation, focusing on granularity and context is required.
3. *Automation*: Enterprise teams must leverage automation for real-time decision making and policy enforcement. This is best done in partnership with a great commercial vendor and TAG obviously recommends that PlainID be included in any source selection for partners in this area.
4. *Logging and Monitoring*: Implementation of robust logging and monitoring mechanisms to capture and analyze API interactions is a key consideration. This is a familiar enterprise security requirement, so transposing this to an API context should not raise any implementation concerns.
5. *Threat Detection*: Security teams must deploy proactive threat detection mechanisms to identify and mitigate potential security breaches. This corresponds to shift-left focus, so any focus on advance indications and warning will provide effective cyber risk management during development.

6. *Third-Party Risk Management*: Exercising due diligence when integrating third-party APIs will help to ensure that external access aligns with internal security policies. This is increasingly identified by API security experts as a requirement since third parties introduce uncertainty in terms of the robustness of their API implementations.
7. *Zero Trust Integration*: Seamlessly integrating Zero Trust principles into the API security frameworks will help ensure continuous verification and authorization. With the reduction of perimeter dependency for most organizations, it is essential that Zero Trust guide design decisions across the board, including for APIs.

HOW PLAINID ADDRESSES AUTHORIZATION AND PBAC FOR API SECURITY

Cybersecurity vendor PlainID supports authorization and PBAC requirements through a commercial offering that modernizes access management and supports dynamic authorization in real time. The PlainID solution is powered by PBAC, which allows enterprises to create, manage, and enforce fine-grained authorization policies for all trusted identities, workforces, customers, and external third parties.[1]

A key component of PlainID's architecture is its Policy Manager, which supports centralized enforcement management in a decentralized enforcement architecture. This provides a focused view to control who has access to what across the enterprise. This function also provides improved visibility of access risks through advanced access control analytics. The result is a means for deploying predictive and prescriptive access control.

The platform also includes so-called pre-built third-party authorizers, which provide access control for authorization enforcement patterns. This is relevant for use in the context of micro-segmented services, Big Data analytic services, API gateways, and other applications. Integrations are included to control authorizations with Istio, Apigee, AWS API Gateway, Okta, Google BigQuery, and Snowflake Authorizer.

The PlainID platform is well-suited to the concept of centralized management of authorization with PBAC based distributed enforcement. Key functions supported in such capability include policy creation, policy investigation, delegated authorization, approval workflows, and audit & governance. All of these tasks support data and data lakes, cloud infrastructure, applications, and identity-related services.

CONCLUDING REMARKS

API security, in the context of effective authorization and PBAC, is characterized by nuanced challenges that demand solid practical solutions. Enterprises must strike a balance between stringent cybersecurity controls and maintaining operational efficiency.

By adopting a holistic approach that encompasses policy development, contextual awareness, automation, logging, threat detection, third-party risk management, and Zero Trust integration, organizations can manage their API security and protect against evolving threats.

As shown in this report, PlainID is an excellent commercial vendor option to support these key requirements for authorization and PBAC. Enterprise buyers working on rationalization or selection of authorization and PBAC vendors are welcomed to be in touch with the TAG analyst team for assistance.

[1] More detailed information on PlainID is available from the company's website where excellent eBooks and reports can be downloaded – see https://www.plainid.com/.

ABOUT TAG

TAG is a trusted research and advisory company that provides insights and recommendations in cybersecurity, artificial intelligence, and climate science to thousands of commercial solution providers and Fortune 500 enterprises. Founded in 2016 and headquartered in New York City, TAG bucks the trend of pay-for-play research by offering unbiased and in-depth guidance, market analysis, project consulting, and personalized content—all from a practitioner perspective.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: Edward Amoroso

Publisher: TAG Infosphere Inc., 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman at lgoodman@tag-cyber.com to discuss this report. You will receive a prompt response.

Citations: Accredited press and analysts may cite this book in context, including the author's name, author's title, and "TAG Infosphere, Inc.." Non-press and non-analysts require TAG's prior written permission for citations.

Disclaimer: This book is for informational purposes only and may contain technical inaccuracies, omissions, and/or typographical errors. The opinions of TAG's analysts are subject to change without notice and should not be construed as statements of fact. TAG Infosphere, Inc. disclaims all warranties regarding accuracy, completeness, or adequacy and shall not be liable for errors, omissions, or inadequacies.

Disclosures: PlainID commissioned this book. TAG Infosphere, Inc. provides research, analysis, and advisory services to several cybersecurity firms that may be noted in this paper. No employees at the firm hold any equity positions with the cited companies.

TAG's forecasts and forward-looking statements serve as directional indicators, not precise predictions of future events. Please exercise caution when considering these statements, as they are subject to risks and uncertainties that can affect actual results. Opinions in this book represent our current judgment on the document's publication date only. We have no obligation to revise or publicly update the document in response to new information or future events.