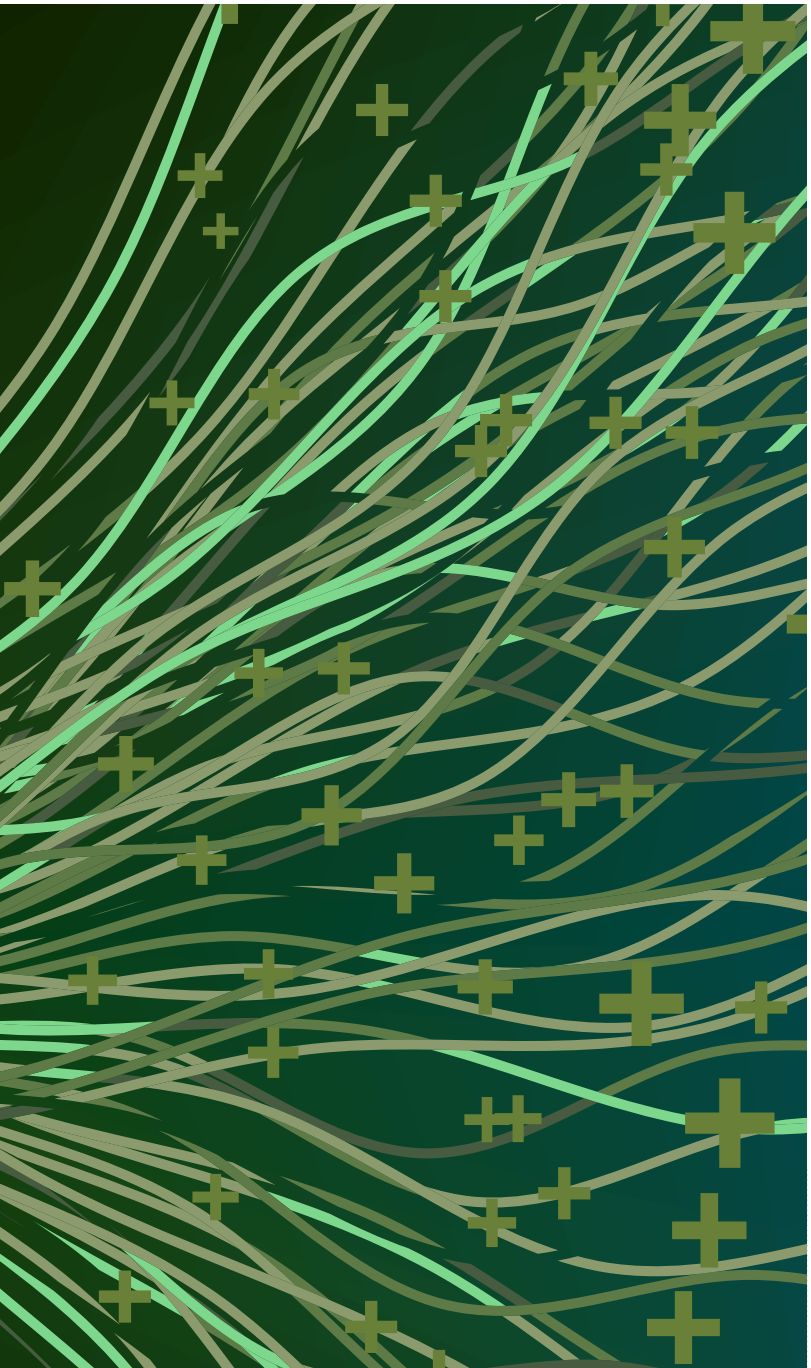
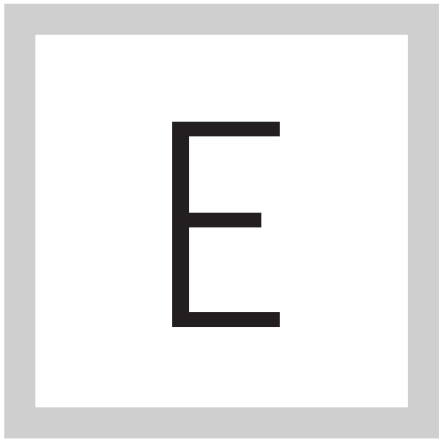


E-Guide

AUTHENTICATION AND AUTHORIZATION: TWO SECURITY ESSENTIALS THAT WORK TOGETHER

TechTarget | SearchSecurity



FFECTIVE IT SECURITY today demands that users be both authenticated and authorized. But even those two steps alone are not enough. Expert Mike Cobb explains.

AUTHENTICATION AND AUTHORIZATION: TWO SECURITY ESSENTIALS THAT WORK TOGETHER

Michael Cobb, CISSP-ISSAP

Authentication is a vital information security control today because is it's the first step in the process of authorization, allowing access rights to be granted based on who a user is. Authentication confirms the identity of someone, or something, while authorization occurs after successful authentication. Authorization then grants or denies read, write and execute permissions on system resources.

ESSENTIAL SECONDARY ACCESS CONTROLS

The logic behind many websites and mobile apps, though, makes the mistake of assuming that, once a user or device has been successfully authenticated and granted the appropriate permissions, further authorization checks aren't necessary. This can lead to apps exposing data to authenticated but unauthorized requests, which negates the benefits of any identity and access management tool.

Home

Authentication and authorization: Two security essentials that work together

The problem arises because developers assume that once a user is authenticated, they can be trusted. Even requests from authenticated users or devices need to be checked to ensure that they are authorized to perform a particular operation. Many developers fail, though, to include these secondary access-control checks. Such checks involve checking the user's permission to view, edit or delete rows and individual fields of the data requested, to ensure the user is both authenticated and authorized to do so.

OAUTH 2.0 IS ONLY A FIRST STEP

Many apps are using the OAuth 2.0 protocol for both authentication and authorization, but technically it's only a specification for delegated authorization, not for authentication. RFC 6749 section 3.1. states:

> The authorization endpoint is used to interact with the resource owner and obtain an authorization grant. The authorization server MUST first verify the identity of the resource owner. The way in which the authorization server authenticates the resource owner (e.g., username and password login, session cookies) is beyond the scope of this specification.

Home

Authentication and authorization: Two security essentials that work together

Although there are many libraries and services that use OAuth 2.0 for authentication, authentication based solely on OAuth is not secure and should be combined with the OpenID Connect standard if developers want to create a secure "social login" that combines both authentication and authorization. OpenID Connect is an identity layer built on top of the OAuth 2.0 protocol. So, whereas OAuth 2.0 permits a user of a service to allow a third-party application to access their data hosted in the service without revealing their credentials to the application, OpenID Connect permits a third-party application to obtain a user's identity information, which is managed by a service. This functionality makes it a lot easier for developers to authenticate their users across websites and apps without having to own and manage their passwords. Google+ Sign-In is one platform based on OpenID Connect and OAuth 2.0 that developers can use to provide a secure social login experience for their users.

AND ONE MORE THING...

Whichever authentication and authorization website and app development teams decide to opt for, it's essential that the associated implementation documentation is read and referred to on a regular basis during development. Although many claim to be simple to deploy, it is a non-trivial job to incorporate

the code and processes securely. Testing should always include both allowed and disallowed misuse and abuse cases, which are unintended and malicious-use scenarios of the application. This is the only way to ensure that authentication and authorization controls are performing as expected, and authenticated users and devices can only perform tasks they're authorized to do so.

MICHAEL COBB, CISSP-ISSAP, is a renowned security author with over 20 years of experience in the IT industry. He co-authored the book IIS Security and has written numerous technical articles for leading IT publications. He has also been a Microsoft Certified Database Manager and registered consultant with the CESG Listed Advisor Scheme (CLAS). Mike has a passion for making IT security best practices easier to understand and achievable. His website www.hairyitdog.com offers free security posters to raise employee awareness of the importance of safeguarding company and client data, and of following good practices.

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.