Advanced Session Security

Countering the Risk of Session Hijacking

ca technologies

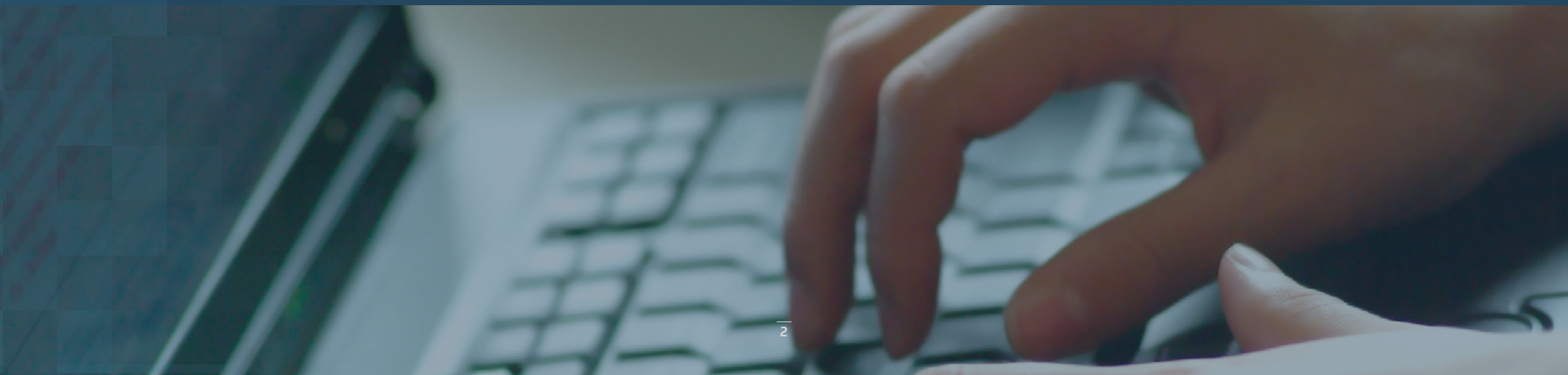
New Technologies Mean New Security Challenges

It's official. We are living in an app economy—one where business users and consumers expect to have full access to their applications and data anytime, from anywhere and on any device. Of course, this trend toward instant access to multiple applications and service providers also generates multiple sets of credentials for users. So, you're under pressure to provide easy-to-use single sign on to further enhance and simplify the user experience.

Convenience comes with concerns

While this paradigm shift has resulted in significantly more convenience for end users, it has created enormous challenges for those of you tasked with keeping your enterprise network and data secure.

Mobile computing and access expanding to applications have conspired to make your static security perimeter ineffective. At the same time, cyber-criminals are becoming increasingly sophisticated and aggressive. The result is a perfect storm of security concerns that you to stay ahead of.



Session Hijacking Is on the Rise Again

In OWASP surveys, IT security experts have identified session hijacking as one of the **TOP 3 SECURITY RISKS** for over a decade.

Source: OWASP Top 10

Data—whether it's obtained legally or not—is the currency of the day. Which explains why enterprise networks are facing an ever-rising number of attacks. It seems like every month brings another high-profile breach, and another unauthorized download of highly sensitive data.

And as users spend more and more time in "sessions," whether interacting with websites or with applications housed in the cloud, you have more doors to guard than ever before. Multi-factor and risk-aware authentication has made gaining network access via stolen credentials increasingly difficult. Which has led hackers to seek other ways into your system—and user sessions are near the top of the list.

Session Hijacking Threats Are Growing in Severity and Prevalence

While session hijacking has never gone away, other threats had gained greater prominence in recent years. Heartbleed and Covert Redirect changed all that. These highly publicized session-jacks refocused IT—and public—attention on this long-time problem that now presents even greater risks.

These days, sophisticated black hats are attacking user sessions from several different directions:

- **Individually vulnerable sites or apps**—Some developers simply fail to build in and maintain sufficient safeguards to protect their users.
- **Predictable session tokens**—Newer decryption algorithms are able to easily break through poor-to-average security.
- **Session sniffing**—A failure to use SSL encryption for traffic beyond login pages lets hijackers intercept session cookies transmitted between the server and the user.
- **Client-side attacks**—Client sites are often vulnerable to Cross-Site Scripting (XSS) attacks, malicious JavaScript code, Trojans and more that put users at risk.
- **Man-in-the-middle attack**—Attackers insert themselves between the user and server so all traffic, including session tokens, flows through them.
- **Man-in-the-browser attack**—The hijacker infects a browser with a Trojan Horse that allows him to alter communications between the user and secure websites.

It takes constant vigilance and continually updated skills to protect users from this onslaught of cyber-crime.

Nearly 75%
of single sign-on administrators surveyed are concerned about session hijacking.

TechValidate Research on Access Management solutions from CA

What Happens During a User Session Matters

The first rule of building session security that offers appropriate protection without unnecessarily impacting the user experience is to accurately assess the sensitivity of the data transaction. Forcing users to jump through hoops to view prices on a retailer's site makes as little sense as leaving a user's stored credit card information unprotected.

Different access and actions carry different risks if data is exposed. Consider these three examples:

Low Risk **Help desk and Meeting Room Manager**

Medium Risk **HR and benefits "read only" documents**

High Risk **Finance and HR/Benefits activity**

In many cases, it's sufficient to authenticate that a user has a legitimate reason to access a site, or a particular section of a site. But, when the user wishes to actively engage with the site, particularly when dealing with sensitive personal or financial information, stronger security is required.

It's your job to **assess each class of interaction and apply security controls** that are appropriate to the potential threat.

Strategies Exist for Preventing Session Hijacking

With so many access points to protect, and no guarantee that users or app and web developers are prepared to do their part, session security can seem like an uphill battle, But, just as cyber-crooks have adopted new techniques over the years, you have new technologies and strategies you can put in place to protect user sessions, as well.

The two most successful methods for enhancing session security are continuous device verification and risk-based authorization. We'll go into greater detail about both in the pages that follow, but to summarize:

- **Continuous device verification** repeatedly reconfirms that the user who initiated the session is still in control.
- **Risk-based authorization** ups the security ante as the user attempts to access more sensitive data, requiring new and more robust authentication before opening the next door.

Both continuous device verfication and risk-based authorization can be extremely helpful in securing user sessions on their own. And when used together they can help you establish a virtually impenetrable shield between your users and the bad guys looking to hijack their sessions.

SESSION SECURITY TIP

Having a secured centralized session is a much better approach to application security than having to manage session security separately for each individual application.

Why Continuous Verification Is Necessary

The problem with session hijacking is that it most frequently occurs without anyone noticing. A black hat gains access to a user's session, and if they are subtle, can manipulate the session without attracting any attention. Alternatively, the hacker just lurks in the background until the user logs off. At that point, the hijacker can take over and gain access to data behind any doors open to that particular user.

The risk is magnified if the user is granted full access after successfully authenticating during log-on. With no further barricades to get past, the hijacker is free to roam throughout the system, unimpeded.

And even when additional authorization checkpoints are in place, the hijacker may still have the upper hand. Because they are recognized to be running an authorized session, she may be able to test, and eventually defeat, deeper security measures without rousing suspicion.

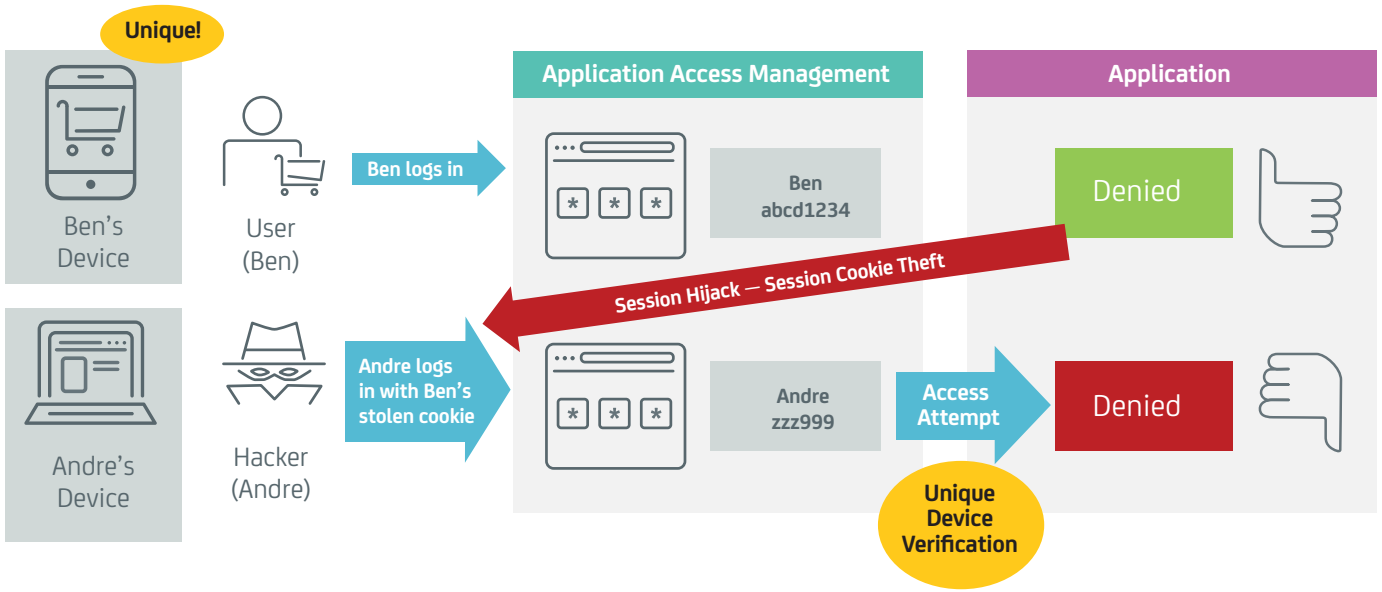
How Continuous Verification Works

To identify and foil hijackers, it's necessary to be able to recognize that the session operator has changed. This where continuous verification techniques come in.

The process begins when the legitimately authorized user logs in and the system captures a unique identifier from the user's device. The system is then instructed to ping the user's device at predetermined intervals, so long as the session remains open.

The continuous verification solution is able to verify whether the same device is connected or not. If, at any time, the device connected to the session fails to verify with the proper identifier, the session is terminated and the connection severed.

Depending upon the frequency of verification, a hijacker masquerading as the session originator can be detected before any damage can be done.



Why Risk-Based Authorization Is Necessary

Again, let's say a black hat passes initial authentication security or gains access to a user's session undetected. The resources that can be exposed pose various levels of threat to your organization. Some may put the most sensitive and valuable assets of your company, customers and colleagues in danger. Clearly one-size-fits-all security protocols make less sense than ever before.

This drives the need for more sophisticated, risk-based authentication at initial login and mandates a risk-aware approach to authorization as well. Once a user has passed initial authentication you can't stop there. By assigning an "access risk score" to every resource, you can set the bar that users have to pass to access all types of resources. For every resource that is accessed, a risk assessment is completed. Requiring minimal authentication for users to access resources with minimal risk potential helps simplify and enhance the user experience. But allowing those same users to migrate into higher risk areas without meeting more stringent authorization requirements opens the door for hackers to do the same.

Using risk-based authorization and the "passing" risk score for a resource gives you the tools you need to enforce stronger authentication for accessing high-risk resources or to altogether deny access.

Access and security rules need to be set appropriately to reflect the potential risk of each type of interaction.

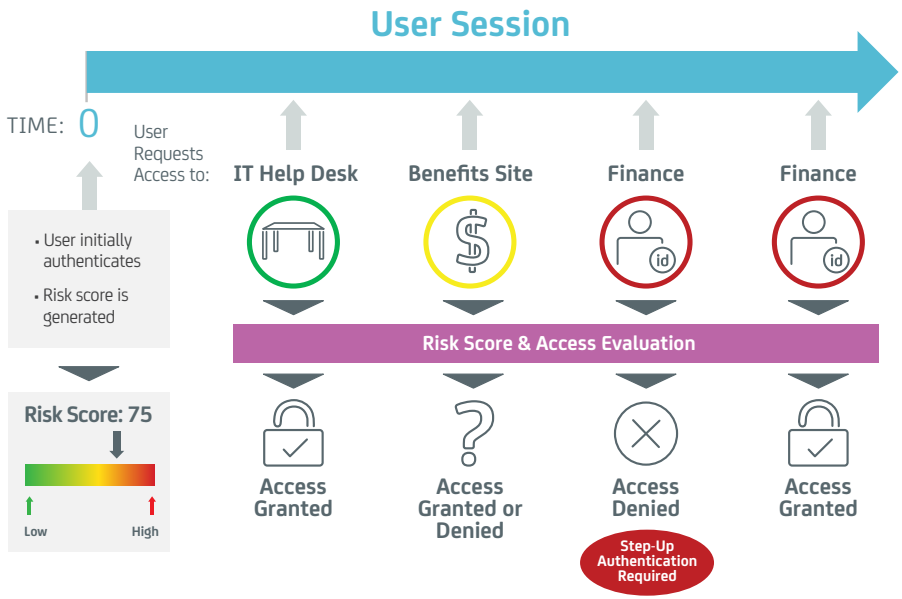
How Risk-Based Authorization Works

To adequately protect your enterprise's data from malicious intruders without unnecessarily inconveniencing users, you need to apply risk-based assessment for access based on the sensitivity of the resource.

Online destinations are assigned risk scores based on the potential threat to the enterprise. Then, when a user opens a session, a risk score is calculated using various factors, including the user's location, time of day and comparison to a behavioral baseline.

Whenever the user's risk score fails to qualify for the location they are trying to access, more rigorous step-up authentication can be required. For instance, a sending a temporary one-time password (OTP) to the user's known email or mobile number offers strong authentication while maintaining a good user experience.

As the diagram shows, a username and password may be sufficient to access the help desk, and possibly some portions of the organization's benefits site. But to get into the finance section of the company's website, where payroll, sales and other sensitive data is available, will require stronger authentication.



Risk-Aware Session Management from CA Technologies Helps to Prevent Session Hijacking

Get the answers to your increasingly complex session security challenges from CA Technologies. Start with **CA Single Sign-On** to control access to resources and deploy **CA Advanced Authentication** to verify user identities at initial login. Then make your session security "risk aware" by combining continuous verification and risk-based authorization to protect user sessions from hijacking threats without overburdening your users with constant interruption.

Learn more about
CA Single Sign-On and
CA Advanced Authentication
at www.ca.com/securecenter

READ THE WHITE PAPER: **"Closing the Biggest Security Hole in Web Application Delivery"**

Learn More About How CA Can Help You Prevent Data Breaches with **Risk-Aware Session Management and Intelligent Authentication Solutions**.

Visit **www.ca.com/securecenter**

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

CS200-152489