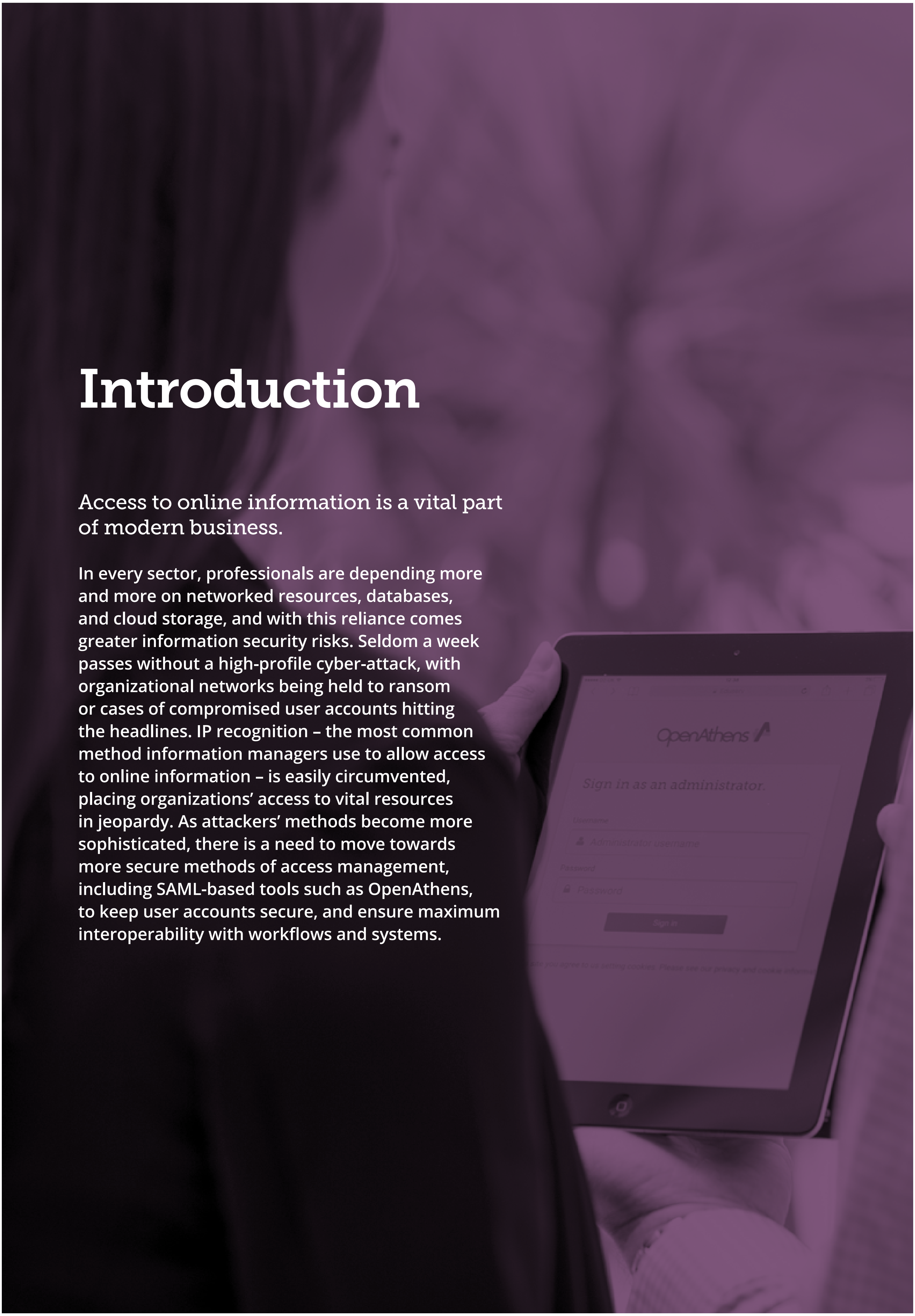
OpenAthens

Approaches to Authentication:

The importance of information security



Introduction

Access to online information is a vital part of modern business.

In every sector, professionals are depending more and more on networked resources, databases, and cloud storage, and with this reliance comes greater information security risks. Seldom a week passes without a high-profile cyber-attack, with organizational networks being held to ransom or cases of compromised user accounts hitting the headlines. IP recognition – the most common method information managers use to allow access to online information – is easily circumvented, placing organizations' access to vital resources in jeopardy. As attackers' methods become more sophisticated, there is a need to move towards more secure methods of access management, including SAML-based tools such as OpenAthens, to keep user accounts secure, and ensure maximum interoperability with workflows and systems.

Old approaches, new demands

The online information landscape is incredibly complex, with essential digital resources present in almost every industry – from academic to corporate research, healthcare to government.

But where subscription-based content is available to the world at large, unscrupulous actors will invariably try to gain access through a variety of methods – anywhere from spoofing IP addresses to using social engineering techniques to obtain legitimate login details.

Most service providers use IP recognition as a primary method of verifying a user's location; while this approach has previously worked to authenticate users within specific organizational communities, it is highly vulnerable to attacks and is increasingly expected to handle authentication scenarios that it was not designed for, nor able to handle without significant workarounds that include additional login prompts, or third-party software to bridge the gap between the point where a user logs in and the content itself that results in a complex or unreliable user experience.

In an environment where users were reliably located within an organization's network, IP recognition worked well as a means of gaining access to secure information such as journal subscriptions – it was a straightforward approach that was widely embraced by institutions and identity and service providers alike. However, as internet access has become more ubiquitous and the amount of information available online has increased, the limitations and flaws of the system have become more apparent – IP recognition serves basic requirements for granting access to resources, but it is not designed from the ground up to address today's challenges of security and transparency, or for the wider variety of usage scenarios that institutions and identity and service providers are asked to support.

> *In working with a variety of publishers, partners, customers, and libraries; we frequently see access to research resources provided to members as a benefit of their affiliation. Part of this arrangement is typically that the institution or library will want to use their membership database to provide access to these resources. IP recognition simply doesn't work in these situations. A comprehensive SSO solution is needed to connect multiple systems. If there is not a SAML based system to carry this authentication, publishers often have to implement stopgap measures or workarounds to prevent unauthorized usage. This results in struggles for the customer as well as an impedance on a good end user experience.*
>
> Timothy Lull, VP of Sales, Software as a Service, EBSCO Information Services

IP recognition also opens systems up to unique security risks: for example IP fraud, where a third party's IP range is added to a legitimate subscription, granting them 'free' access to those resources without the knowledge of either the publisher or subscribing institution.

Due to its reliance on the user being within a physical network environment, or using proxy services (where traffic from within an organization is routed through a single IP address) to emulate that environment, IP authentication limits the mobility of your users which can in turn encourage bad behaviour like the use of open proxies, as well as severely

Key terms

Identity provider: An organization or product that confirms user identities and attributes to enable them to access content owned by service providers. Examples of IdP products are OpenAthens, Shibboleth and Ping Federate.

IP Address: A numerical reference (e.g. 123.123.123.0) that identifies the location of a device on a network or the wider internet, managed globally.

IP Authentication: A form of access management that grants access to resources by recognizing the IP address of a user's device.

Proxy Service: Software that acts as an intermediary between users and content. Often used to facilitate remote access to subscription- based content.

SAML: 'Security assertion markup language'. A protocol for exchanging security information between identity providers and service providers.

Service provider: An organization that provides content or services.

SSO: 'Single sign-on'. Providing users with access to many different systems through a single set of login details.

limiting traceability. This can prove to be a problem if you need to investigate cases of persistent misuse of resources from an IP within your organization. Without further transparency, it is difficult – if not impossible – to track that misuse to an individual's actions.

These limitations around tracking usage and gaining insight into user activity can also prevent making more informed purchasing decisions. In particular, proxy services make it impossible to track usage beyond the top-most level within a network, resulting in a lack of granularity that has serious ramifications for businesses that need to allocate subscription charges to particular cost centers. Further issues arise if there is more than one subscribing organization within an IP range, such as hospital groups; in these cases, IP authentication is not able to manage licenses for each individual institution. There is a similar problem if the subscribing organization has dynamic IP ranges in place.

Aside from fraud issues, other issues exist in that sometimes IP address are inaccurate or a range is too wide, and this can let in other institutions that the publisher hasn't authorized. Our licenses – and I'm sure, that of other publishers – have an appendix that ask the customer to specify all institutions that will gain access as part of their license, and all IP addresses linked to those institutions, but this data isn't always completely accurate. It's not just institutions, though: publisher data can also be very messy when it's been compiled from various systems.

We're in the very early stages of moving from IP recognition, but I think it will be replaced by a SAML-based approach. I think it should reduce a number of access problems on both sides – institutions losing access, or gaining access they shouldn't have – and reduce administration overheads.

As well as IPs being inherently insecure and something of a blunt instrument, moving to other methods of authentication should also give us all a better view of usage data – for example, identifying where usage hotspots are so we can better support institutions that have access as part of a regional or national deal.

Keith Abbott, Special Projects Manager, Wiley

Rethinking authentication

There are a number of alternatives to IP recognition-based systems, such as OpenAthens, which make use of a SAML-based single sign-on approach to connect users with content.

Not only do these have the benefit of reducing friction for users – once they have signed into their account, they have seamless access to their institution's resources – but the additional level of security also is important in keeping these connections secure.

> *SAML is a standard that is used to exchange information (attributes) about users with the resources they are accessing while keeping their login details private. SAML is well-established and widely-deployed and uses industry standards and best-practice to digitally sign and encrypt messages to prevent fraudulent use or interception by attackers. Furthermore, most SAML-based systems, such as OpenAthens allow granular control over what attributes are exchanged with particular resources. This makes SAML not only a more secure alternative to IP recognition but also a more flexible framework for SSO for many different scenarios.*
>
> David Orrell, Systems Architect, OpenAthens

Information security goes beyond the software aspects of an authentication service, as any solution is only as robust as its weakest point – measures need to be in place to protect the administration systems from potential compromise, too. As such, as well as OpenAthens' industry-leading secure code base, Eduserv has obtained ISO 27001:2013 certification covering all aspects of its networks, premises, and services to ensure best practice is followed in protecting the infrastructure and administrative accounts that organizations rely upon to grant access to content.

> *Identity and Authentication are critical blocks in building in trust and accountability in transactions. In today's world IP authentication alone provides little assurance to either party. OpenAthens uses established open standards to build multilateral trust and veracity.*
>
> James Mulhern, Chief Information Security Officer, Eduserv

As well as keeping administrative accounts secure, OpenAthens also includes tracking systems to help identify potential misuse of user credentials – including unusual activity spikes, and potential sharing of login details. Support teams stay in constant contact with institutions and publishers to identify any issues and address them as early as possible, helping keep accounts secure and ensuring that the terms of subscription agreements are met.

> *A publisher reached out to us to explain that a particular user ID from a specific organization had downloaded an unusually high amount of content from their platform and had blocked access for that specific account. Through checking our logs we were able to provide the organization with the necessary information to track down the individual, investigate and take necessary actions. Had this organization been using IP recognition the entire organization's access would have been disabled instead of that particular user, and it would have been extremely difficult for the organization to identify the user in question.*
>
> Adam Snook, Technical Pre-Sales Consultant, OpenAthens

Because OpenAthens is based on standard frameworks, it is also more flexible than many other solutions, allowing for seamless

interoperability with discovery and library portal systems, and a more consistent user experience – particularly with single sign-on support across networks and devices.

> *I've helped many libraries over the years to review and renew their technology infrastructure and I still see a lot of frustration around the lack of single sign-on; it disadvantages library access to scholarly content. Getting this done properly, especially for off-campus access, is very significant for end-users. If they hit barriers they seek other routes to scholarly content that don't involve the library.*
>
> *Tackling authentication properly through SSO allows libraries to provide publishers with an assured secure channel between users and content. More importantly it makes for an improved user experience that will encourage researchers and students to use that route and not risk channels that are insecure or of dubious legality.*
>
> Ken Chad, Ken Chad Consulting Ltd

SAML authentication in conjunction with a personal ID has a further benefit to end-users in the form of personalization. With this approach, the content and even design of a service can be tailored to suit each individual user's needs. In the same way that OpenAthens allows publishers to identify abuse of access – highlighting those who are bulk downloading or scraping information – a personal login allows publishers to save individuals' previous searches and present semantically-targeted information (for example, returning lists of related content based on previous reading) that can help users discover a wider range of information.

Keeping content and users protected

As the limits of IP recognition are increasingly exposed from both a usability and security point of view, more secure standards such as SAML-based SSO are emerging as the best way to ensure services are protected against misuse, as well as conforming to best practices that meet contractual expectations around securing access to information resources.

They also provide greater transparency of how collections are being used to help libraries make more informed budgetary decisions, and a superior end-user experience regardless of whether they are accessing resources from within an institution’s network or on the go.

Are your systems secure?

If you'd like to find out more about OpenAthens, or to arrange a demonstration, contact us today:

www.openathens.org/contact-us

OpenAthens Sales: **+44 (0) 1225 437 514**

Email: **openathens@eduserv.org.uk**

References & further reading

Abbott, K., White, C., Pitts, A. – *Who's reading your valuable content, and did they really pay for it?* UKSG 2016 conference breakout session, accessed 17th August 2016.

www.slideshare.net/UKSG/uksg-conference-2016-breakout-session-whos-reading-your-valuable-content-and-did-they-really-pay-for-it-keith-abbot-charles-white-and-andrew-pitts

OpenAthens Identity and Access Management Glossary, 26th October 2016.

www.openathens.org/glossary

Ochs, J. – *Guest Post: The American Chemical Society on the Shared Cybersecurity Concerns of Universities and Publishers*. The Scholarly Kitchen blog, accessed 17th August 2016.

https://scholarlykitchen.sspnet.org/2016/06/17/guest-post-the-acss-jack-ochs-on-the-shared-cybersecurity-concerns-of-universities-and-publishers/

Taylor, M. – *Does Sci-Hub phish for credentials?* Sauropod Vertebra Picture of the Week blog, accessed 17th August 2016.

https://svpow.com/2016/02/25/does-sci-hub-phish-for-credentials/

Parley, R. – *Single sign-on access: a more user-centric vision*. Research Information, published 25th September 2015, accessed 17th September 2016.

www.researchinformation.info/news/analysis-opinion/single-sign-access-more-user-centric-vision?news_id=1988

About OpenAthens

The team at OpenAthens develops and supports identity and access management software. Its mission is to remove barriers to knowledge and connect people to information. Over 2,000 organizations use the software, equating to a worldwide network of millions of end-users. The OpenAthens international customer base includes a large number of universities in the UK and beyond, medical and national health organizations, major corporate research organizations, and some of the world's largest publishers.

Contact us at:
openathens@eduserv.org.uk
or by phone at
+44 (0) 844 5000 115

www.openathens.org