International Journal of scientific research and management (IJSRM)
\||Volume||3||Issue||6||Pages|| 3180-3187||2015||
Website: www.ijsrm.in ISSN (e): 2321-3418

Authentication Revolution using Bring Your Own Identity

Supriya N. Kolambkar[1], Prof. RakeshSuryawanshi[2]

[1]PG Scholar, Dept of MCA, A.C Patil College of Engineering, Navi Mumbai, India.

[2]H.O.D, Dept of MCA, A.C Patil College of Engineering, Navi Mumbai, India.

Abstract— With the growing acceptance of cloud-based services, it is becoming less important where an identity access management (IAM) system actually resides. Proponents of BYOID maintain that traditional identity provisioning is no longer necessary and allowing a third party to assume the security, privacy and compliance burdens associated with IAM reduces administrative overhead, simplifies data management and lowers storage costs. Adversaries warn that BYOID has too many risks, including the potential for compromised identities and identity theft. In the enterprise, BYOID may be called identity as a service (IDaaS). IDaaS for the enterprise is typically purchased as a subscription-based managed service that provides subscribers with role-based access to specific applications or virtualized desktops through a secure portal.

Keywords— Information Security, Digital Authorization, One-time Authentication, Self-care Transaction, Digital Identity, Encryption and Decryption, Identity Access Management

I. INTRODUCTION

As people become more accustomed to online social network interactions, they are starting to expect the social experience to be more integrated into online access for their personal financial institutions, government, and other enterprises.

BYOID (bring your own identity) is an approach to digital authentication in which an end user's username and password is managed by a third party such as Facebook, Twitter, LinkedIn, Google+ or Amazon.

BYOID is increasingly being used for website authentication. Instead of requiring visitors to create a new username and password during the registration process, the website allows visitors to use their existing social identities such as Facebook, Twitter, LinkedIn, Google+ or Amazon to log in.

II. Overview of BYOID

2.1 BYOID Open Standards:

Security open standards are developed primarily for vendor interoperability, and this aspect is most important in the arena of large social and cloud vendors.

There would be simply no way that these services could provide the value that they do without reliable interoperability standards. Similarly, in a B2C Open Standards used are as follows:

- **SAML (1.x-2.x):**

Security Assertion Markup Language is a standard to achieve user identity and provisioning. It documents on-the-wire protocol standards for exchanging authentication data between secure domains; that is, between the user and process that provides the identity (a producer of assertions) and a service provider (a consumer of the assertions).

- **OpenID:**

An open standard that describes how users can be authenticated in a decentralized manner. It provides a way for users to consolidate their digital identities by having a single OpenID when connecting to different websites. Effectively, it eliminates the need for services to maintain the password for an identity locally.
The primary difference between SAML and OpenID is that SAML mandates a federated trust between the Identity and Service providers, prior to a system being available, whereas OpenID does not. There are other differences, but these are the major ones.

- **OAuth (Open Authorization):**

An open standard that provides delegated authorization. It offers a way for users to share personal resources on a resource-hosting site with a third-party entity in a delegated fashion. In this

environment, adoption increases if legal and business agreements between entities are not required.

2.2 BYOID Capabilities :

Open standards that are leveraged to implement the BYO-ID capabilities include:

- Point of contact for web security
- User self-care
- One-time password authentication service

a) **Web Security:**

Web Gateway provides a web reverse proxy security solution with centralized user access management to deliver highly scalable user authentication, authorization, and audit services to web applications

b) **User Self-care**:

The User Self-Care (USC) capability allows users to self-manage online accounts

c) **One Time Password Authentication Service**:

Common OTP integration patterns have already been implemented using email, 3G/4G Short Message Service, and HMAC, or software-based tokens such as Google Authenticator.

TABLE I. USER SELF CARE OPERATIONS

User Self-Care operations	**Descriptions**
User registration	User can establish an account on the Internet by executing the enrollment workflow.
User ID existence check	On the initial enrollment page, a button is provided for the user to click to determine whether the user ID entered in an associated field already exists in the registry.
Password change	Can be user-initiated to perform password change operation or auto-initiated due to password expiration.
Forgotten user ID	To recover the customer's forgotten user ID.

standard, a user's authentication information (for example, password) is never shared with this third-party entity.

2.3 BYOID Implementation Patterns:

A typical web user today has too many online accounts and too many usernames and password combinations to manage. At times, the thought of needing to register a new account for a website can be seen as one too many.

Fortunately, many websites today are recognizing this and are moving quickly to embrace the pattern of BYO-ID. This pattern lets customers use their existing online identities from popular online identity providers to authenticate with little or no registration process.

TABLE II. SOCIAL NETWORK SUPPORT FOR OPEN STANDARD

Social Network	**Relevant Open Standard**
Facebook	OAuth
Twitter	OAuth
Yahoo	OpenID
Google	OpenID and OAuth
LinkedIn	OAuth

Authentication Using Social Media:

Authenticating to a website using BYO-ID brings a range of benefits to both customers and the enterprise (or service providers):

a) By allowing consumers to utilize their existing online identity from Facebook or Twitter to authenticate to a website, it results in users needing to remember or manage one less password or one less account.

b) For service providers, BYO-ID results in having very minimal account administrative responsibility by eliminating the user account provisioning process and on-going password management operations. In cases where the enterprise wants to reduce the registration overhead, they can pre-fill information that would otherwise need to be typed. This also allows the enterprise to capture additional authentication data, such as Q&A and mobile phone number, so that the service provider

Forgotten password	To recover the customer's forgotten password.
Account deletion	To deactivate or delete the customer's Internet account.

2.4 BYOID Authentication Workflow:

The workflow is based on the concept of allowing customers to indirectly authenticate to their target website (service provider) with their existing account from a chosen identity provider.

Effectively, the authentication process is delegated to the chosen identity provider. As far as the user is concerned, they are only aware of using their online social identity to log in. Consequently, the credential issued by the selected identity provider lets them seamlessly authenticate to the targeted enterprise website.

More technically astute users would be aware that under the covers there are registries that exist within the service provider that stores the account information (but not the password); this provisioning aspect is not shown in Figure 1

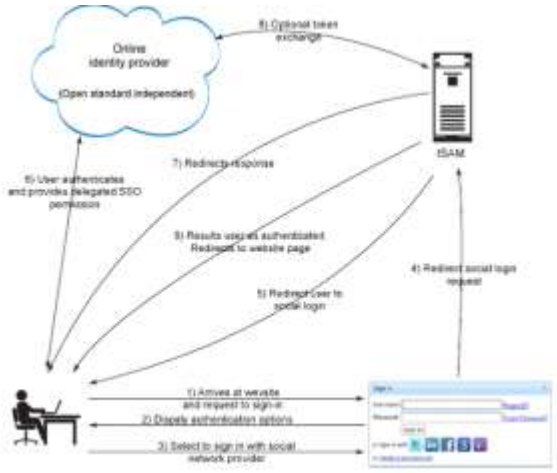

Fig. 1. BYOID Authentication Workflow Overview

III. **Current Global Status of BYOID**

Customers engaging with the business via the Web and mobile devices are the highest rated for targeted digital identity engagement, eclipsing other populations such as job recruits, employees, contractors and retirees.

This interest in mobile customers reflects the continued growth of mobile apps and devices as an increasingly popular way for customers to engage with organizations. Moreover, respondents probably see BYOID as greatly simplifying the user experience on mobile devices.

may invoke higher levels of authentication.

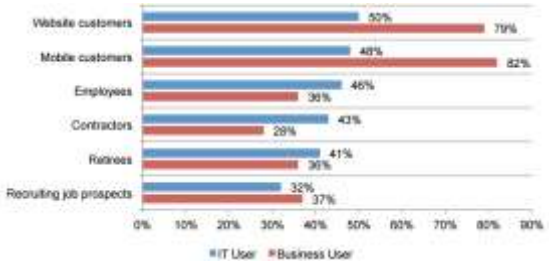

Fig. 2. Level of Interest in accepting digital identities

IV. Preferred Digital Identity Providers

Respondents were asked to prioritize a list of identity providers for use as both an individual consumer and for use at their business.

As shown in Figures 3 and 4, IT users rank PayPal, Google and Amazon as their employers' top three preferred identity providers to their organization.

Yahoo was ranked the lowest priority. The same IT users ranked Google, LinkedIn and PayPal as their personally preferred identity provider for accessing services as individuals.

Fig. 3. IT Users rank Identity Providers
NOTE: 1=most interest 7=least interest

Fig. 4. Business Users rank Identity Providers
NOTE: 1=most interest 7=least interest

V. Legitimate risk and liability concern

While BYOID delivers business value, it is not without risk and liability concerns that may inhibit broader adoption. First, some business users still resist utilizing a third party identity due to privacy concerns and a need to maintain anonymity.

Some are also concerned about using a third party identity for certain transactions or scenarios. They might be perfectly satisfied with using social login to access a newspaper, but will not do the same to access their online banking account.

Organizations that accept third party identities also worry about instances where an identity is compromised and non-legitimate access is granted to applications or customer data. This adds to the complexity of how liability is handled in the event of a data breach or compromise.

Thirty-four percent of IT users say risk/liability concerns followed by complexity (21 percent) and loss of control (19 percent) are barriers to deployment. When asked to identify the most significant inhibitor to BYOID deployment in their organization, 31 percent of business users cite cost, followed by complexity (23 percent) and risk/liability concerns (19 percent).

VI. Identity Validation Process increase Adoption

When asked to identify which features would most likely increase BYOID adoption within an organization, IT users cite the following: the identity validation process (73 percent), multi-factor authentication (66 percent) and fraud risk engines (57 percent) as greatest areas of interest.

In comparison, features business users are most interested in include: identity validation process (71 percent), simplified user registration (71 percent) and fraud risk engines (37 percent).

Features most likely increase BYOID Adoption:

- Identity Validation Processes
- Multi-factor Authentication
- Identity provider implementing fraud risk engines
- Simplified user registration
- SMS mechanisms for user validation
- Simplified password or account recovery
- Risk based evaluation of account recovery

Business users prefer to add passive factors such as geo-location tracking. This is consistent with the overall theme in this survey around simplifying the user experience as passive factors do not require minimal action by the end-user, yet can still reduce risk.

VII. Digital Identity Characteristics

Both groups identify other information that would be valuable to organizations accepting digital identities having access to other data from the identity provider such as history of password resets and account abuse are of greatest interest as this data can help identify potentially fraudulent activity.

Since frequent password resets attempts could be evidence of a compromised or hacked account, this data indicates that both business users and IT users agree that password reset data could be helpful for fraud detection purposes.

Characteristics known to Identity Provider:

- History of password resets
- Abuse account use
- History of identity takeovers
- Length of user account lifetime
- Account suspension notification
- Token expiration
- Account recycle notification

VIII. Reasons to adopt BYOID in Organization

IT users are primarily interested in using BYOID to combine digital identifiers owned by each BYOID user to create a stronger identity credential (69 percent of IT users). By contrast, the most popular reason for business users to adopt BYOID is to capture attributes about individuals from external sources (89 percent)

Reasons to adopt BYOID in Organization:

- To combine digital identifiers owned by each user to create a stronger identity credential
- To outsource password reset activities to identity providers
- To get multi-factor authentication at a low cost
- To capture attributes about users from external sources

processes and user identity

To increase control or scrutiny, both the majority of IT users and business users would like to have mobile device factors added to the digital identity. IT users would also like 4-digit PINs and risk-based evaluations.

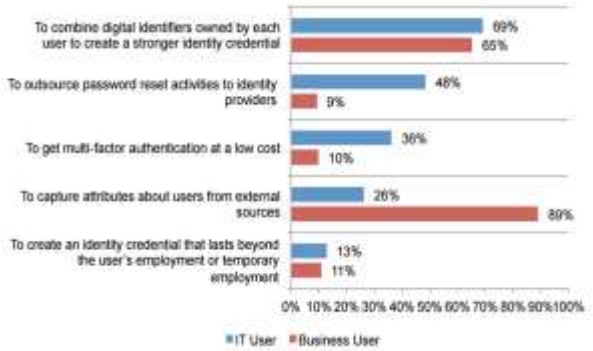

Fig. 5. Reasons to adopt BYOID in organization

IX. Benefits of BYOID within Organization

Both IT users and business users view the ability to streamline the user registration process for customers as the most convincing case to adopt BYOID. Business users second highest priority BYOID use case is to access additional identity attributes for targeted marketing purposes.

Benefits of BYOID within organization:

- Streamline online user registration process for new customer acquisition
- Support for specific mobile initiatives
- On-boarding of employees
- On-boarding of contractors
- Accepting social identities to access additional attributes that drive targeted marketing promotions

Fig. 6. Benefits of BYOID within organization

X. Use of Digital Identities

IT users and business users can have following

- To create an identity credential that lasts beyond the user's employment or temporary employment

- Strengthens the authentication process:

With the rapid growth of networked systems and applications such as e-commerce the demand of effective security is increasing. Most systems are protected through a process of user identification and authentication.

Authentication provides secret and private user information which can authenticate the identity. Authentication approaches can be classified into three types according to the distinguishing characteristics specified in figure 7.

a) What the user knows – Knowledge-based authentication (e.g., password, PIN, pass code)

b) What the user has – Possession-based authentication (e.g., memory card and smart card tokens)

c) What the user is – Biometric-based authentication; physiological (e.g., fingerprint) or behavioral (e.g. keyboard dynamics) characteristics

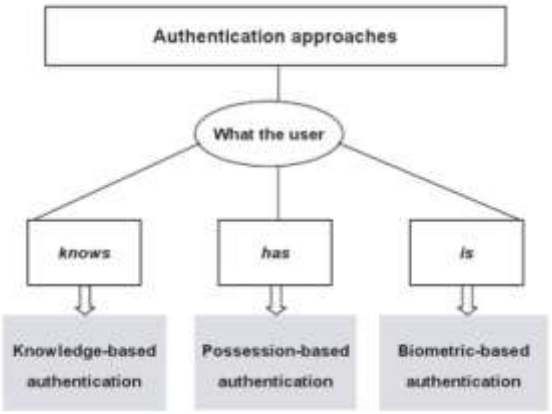

Fig. 7. Classification of authentication

- Reduces the cost of insecurity:

Issues of potential invasion of privacy is raised when such information willingly provided by the visitor to website is subsequently matched against other commercially available sources of information (e.g. demographic to build a more detailed profile of individuals which is stored in electronic databases and which may be made available to other parties)

aspects of having digital identities that will add values to organization:

- Delivers a better customer experience:

User can use single credentials to all the transactions on different websites will bring them to great experience with ease of hand on different transactions. This will lead to great customer satisfaction and trust on digital identity provider

- Streamlines operations and logistics:

All the operations are performed on single account and preferable to deliver product on specified details of user

- Increases employee/user productivity:

Users are interested in single account transactions rather than using multiple login id and password for different websites

- Enables self-service processes:

Registering on third party digital identity provider, User is creating a self identity for the transactions which can make him to authorize himself for each and every transaction

- Decreases customer turnover:

Businesses lose customers all the time. It might be the fault of the business that the customer has no need for the service anymore, or that he or she moved to another area and cannot shop at the same business.

This process of losing customers and gaining new ones is known as customer turnover. Gaining new customers is harder and more costly than keeping old ones, so businesses tend to focus more on keeping the customers they already have.

- Increases the effectiveness of marketing activities:

Keeping the name of the business in front of its customers means a healthier bottom line and a business more likely to survive in the long run.

Marketing centers on the customer, which means there are nearly as many different types of marketing as there are types of customers. BYOID thus brings more effectiveness for such marketing activities to sustain existing customers.

- Increases customer acquisition:

To gain new customers through targeting them and reaching them through online and offline customer journeys is very toughest task. And it helps to reduce customer acquisition cost.

- Enhances innovations in products and services:

Innovation is a key to growth, to acquiring and sustaining competitive advantage, and to building shareholder value for the long term. At the same time, the innovation process is fast becoming more open, and more global: Setting up shop in local markets around the world and getting customers more involved in innovation efforts are now a vital part of any successful innovation effort.

- Generates new revenues:

There must be some ways for you to generate additional revenue at your venue. In the highly competitive events industry, venues are constantly looking for ways to decrease dark days and to use available resources to increase revenue. Here are four ways the most successful venues generate new revenue streams.

1. Market your venue for use by nontraditional events:

Traditional events need space, too. Arenas that are configured for the task should market their space to conferences. Convention centers should target performance events.

2. Offer more services to your clients that would normally come from a third party:

Build relationships with new vendors so your organization can receive a percentage of what happens in your building while they coordinate the services.

Or become the vendor yourself and offer services such as online and onsite registration to organizations planning events at your venue. Your clients will appreciate your one stop shop services.

3. Sell targeted sponsorships or ad space to companies for specific events:

Digital signage and menu boards can be used for more than just communication. Sell digital rotating ads or logo placement targeted to specific events.

4. Produce your own events

A thorough evaluation of marketplace and creating an event that targets new customers for customer acquisition. This will help you in keeping more of the revenue from events that happen in your venue by generating events without the help of a third party

planner.

XI CONCLUSIONS

In today's application economy, the old network perimeter is no longer relevant—today's IT organizations must deal with highly distributed identities across the entire business environment that come from many sources.

In addition, mobile employees and customers are redefining the challenge of delivering secure access to applications quickly. Users need to be able to access information anywhere, anytime, and from a range of different devices. These factors cause a dramatic shift in the role of security and how user identities should be managed.

Previously, managing digital identities was traditionally viewed as a cost center. However, the rapid proliferation of web and mobile applications has transformed managing identities from a cost center to value center.

BYOID is a promising trend that offers simpler user engagement and acquisition without significant infrastructure or management costs. As the findings of this research reveal, the level of interest in BYOID indicates that this trend has traction among IT and the lines of business

This means that organizations should begin assessing how BYOID fits into their organization's long-term plans. To achieve BYOID adoption, organizations should encourage greater cooperation and collaboration between IT users and business users. The purpose should be to align the business goals in a manner that leverages BYOID without sacrificing security or increasing risk exposure to an unacceptable level.

Consummating this IT and business collaboration around BYOID can help organizations successfully grow and meet new business initiatives. In the short term, organizations should consider taking these three concrete steps to assess if and how BYOID would fit into the current organizational strategy:

1. Engage IT and business in collaborative discussion around BYOID. Your organization may already be utilizing BYOID for some specific initiatives, but to monitor BYOID trends. BYOID continues to be an active area with new developments both from vendors and public/private sectors. Some of these developments fall into enhancement of existing standards, and they also cover a lot of the business enablement and risk/liability issues
2. Achieve maximum gain, organizations should conduct an overall assessment of current and future business initiatives to determine potential fit for BYOID. This exercise could include basic simulation/modeling of a new online initiative with BYOID and without BYOID.

   Conduct BYOID risk assessment. An important first step would be to convince a cross-functional team with business, legal and privacy expertise to understand the underlying risk and liability issues. This may require engaging with an outside firm or auditor. Given that online users could literally be from all over the world and subject to a wide range of privacy regulations, it is important to understand the risks involved so business can make best decision around BYOID.

3. Conduct BYOID risk assessment. An important first step would be to convince a cross-functional team with business, legal and privacy expertise to understand the underlying risk and liability issues. This may require engaging with an outside firm or auditor. Given that online users could literally be from all over the world and subject to a wide range of privacy regulations, it is important to understand the risks involved so business can make best decision around BYOID.

that were covered in this report. Leveraging other industry work in BYOID can help enhance your own efforts and ensure that best practices are always being utilized.

REFERENCES

[1] Bart Preneel, Demosthenes Ikonomou , Applications to encrypted databases; the study of video surveillance architectures and new networking concepts and innovative solutions for identity management, APF 2014, Athens, Greece, May 20-21, 2014

[2] Jannie Zaaiman, Louise Leenan, The Proceedings of the 10th International Conference on Cyber Warfare and Security, Academic Conferences Limited, 24-Feb-2015

[3] John G. Iannarelli, Michael O'Shaughnessy, Information Governance and Security: Protecting and Managing Your Company's Proprietary Information, 09-Sep-2014

[4] Ponemon Institute LLC, Moving Beyond Passwords: Consumer Attitudes on Online Authentication - A Study of US, UK and German Consumers, 2013

[5] Christopher Hockings, Jenny Wong, Enable bring-your-own-identity authentication
Leverage security open standards using social networks to manage identity lifecycle operations

[6] Zack Martin, Cutting Edge: 'Bring Your Own Identity', 06 August, 2014

[7] Doron Cohen, Bring-Your-Own-Identity (BYOI) – Bring It On, December 19, 2013

[8] Ellen Messmer , Is "Bring Your Own Identity" a security risk or advantage?, Jul 28, 2014