Biometric Integration in Web Applications: Security for Web Apps

DANNY THAKKAR | CLOUD-BASED BIOMETRICS, SINGLE SIGN ON

Today, web applications have claimed a significant chunk of market share from their aging counterparts such as client-server and locally installable applications. It has become possible due to some unique advantages that web applications offer. Assessable via web browsers, they can work as good as locally installable applications without installing and maintaining them. The fact that organizations do not have to allocate resources to maintain them locally, has also accelerated the adoption of web applications.

Many other factors also helped web applications to become widespread and attractive to business as well as personal users. Advancements in web development technologies, increasing internet accessibility, higher bandwidth, competitive subscription prices and big players such as Google, Amazon, Microsoft, etc. getting involved, has helped web applications to attain their present status.

Web applications have greater need of security as they are assessable from anywhere with a URL. Unlike locally installed applications, in which information systems can also be secured with physical security accesscontrol, web applications do not have this advantage.

Now with the rise of new technologies, standards and APIs, it has become to leverage other means of information security like biometrics, USB token, YubiKey, etc.

The subsequent sections of this article further discuss about web applications, web based biometrics and integration of biometric authentication in web applications.

Evolution of web applications and biometrics

Early days of computing were dominated by client-server and standalone applications. Software applications were either deployed in a client-server environment or installed on the standalone systems. It was important to keep things 'local' back then.Locally installable applications, local network, local storage options, local processing power, etc.were the way to go.However, things were bound to change with the emergence of the World Wide Web.

When the World Wide Web started to take shape in early 1990s, it was mostly a collection of static pages. Designed mostly with the HTML, Web pages were more or less like documents that were accessible via the internet. They were nowhere dynamic or interactive as today's web pages.When users clicked any link on the web page, the request would return to the server and reload the entire page. For example, clicking "Show more" link at the bottom of a page would reload the entire page, instead of just showing rest of the content / page. Some level of interactivity was made possible by the sequence of pages. Passwords were the digital security guards of the new-born WWW.

In 1995, when Netscape introduced Java Script, a highly popular client side scripting language, some dynamic elements could be programmed that loaded with the webpage. Java script elements could perform some actions locally instead of reloading the entire webpage on each request.

In 1999, with the introduction of Servlet Specification version 2.2 in Java and Ajax in 2005, it became possible to create more dynamic and interactive web pages. Use of Ajax techniques allowed webpages to send and receive data in the background, i.e. without reloading the entire page and distracting the user interface. This was an important milestone in the direction of web applications as they need high level of user interactivity.

As the web evolved, biometrics also evolved alongside. By 1999, biometric researchershad set some major milestones. It was the year when FBI's IAFIS (Integrated Automated Fingerprint Identification System) became operational. Before that in 1997, first commercial, generic biometric interoperability standard had already been published. However unlike the web, which was invented in 1989, history of biometrics is more than 100 years old.

Web-based biometrics: biometric authentication in web application

Web based biometrics is an approach, in which biometric authentication is programmed to take place on the web. Web based biometrics enable users to authenticate with their biometric identifiers to login to a web resource accessible via a browser. This approach of authentication can be utilized by web applications, email accounts, or many other secure resources on the web, which require user authentication before granting the access.

Since web based applications reside on their host server and load in a web browser when requested, it is the browser they have to rely on to access the local hardware resources as well as the external devices. So the web browser works as the mediator between the resources on the local machine and the web application.

When it comes to the web based biometrics, this ability is provided with the use of APIs. APIs are discussed in details in the section – How to integrate fingerprint scanner with web application?

Web applications work like an on-demand, online software, which can be accessed via a web browser.Users do not have to entangle in managing different aspects such as installation, minimum hardware requirements, configuration, compatibility, etc. All you need is a compatible browser and the rest can be taken care of by the service provider.

Organizations are now ditching client-server as well locally installable standalone applications in favour of web apps. Even non-business users are also choosing web applications for their ready-to-use nature. This shift is hardly surprising as web applications' list of advantages hugely outnumber their drawbacks.

However, despite this huge shift and unprecedented growth of web apps, they still rely on passwords for account and information security.As personal as well as business computing needs shifts towards the web applications and cloud computing, biometric authentication in web applications (e.g. web-based fingerprint authentication) now makes a perfect sense.

Use of web-based biometrics to enable biometric authentication in web application offer unique advantages like:

- No need for software installation
- Less storage, memory, and processing resource consumption on the client
- Reduced IT Management costs
- Automatic software updates
- Desktop platform independence
- Better security
- Authentication and authorization capabilities
- Reduces license costs while effectively increasing license utilization
- Simplifies deployments

How to integrate fingerprint scanner with web application?

Most biometric hardware manufacturers offer APIs (Application Programming Interface) to allow developers to integrate their custom applications with biometric readers. APIs enables developers to access and integrate services or hardware with their solution without starting the integration process from scratch. For example, SecuGen Web API, Aware's Next|Fingerprint, etc.

These proprietary APIs are generally designed for a particular product range offered by the manufacturer, so they will not work products from the other brands. These APIs contain specific code and instructions that enables the biometric hardware (i.e. fingerprint / face / iris / other biometric readers/scanners) and user agent (i.e. browser in case of web application) to interact with each other.

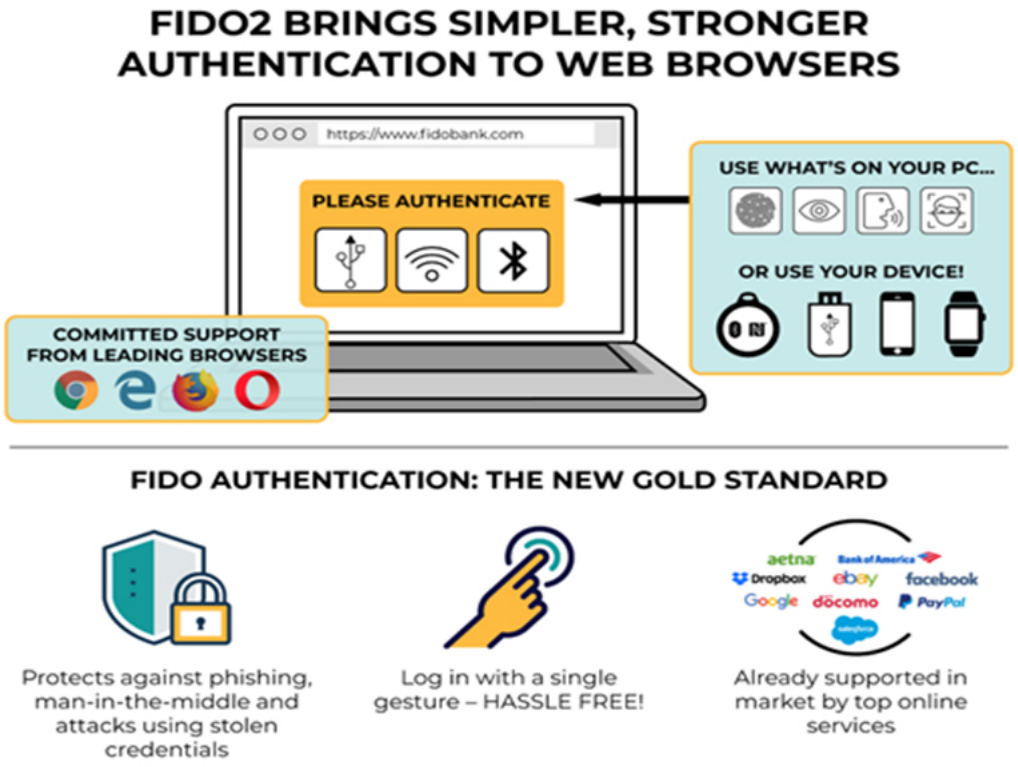

Image: WebAuthn API allows users to create and use public key cryptography based authentication methods such as biometrics, USB token, etc. (Image Credit: w3.org)

In April 2018, FIDO Alliance and the World Wide Web Consortium (W3C) announced to have a major standards milestone achieved. The new standard called WebAuthn is expected to bring stronger yet simpler web authentication to the table. WebAuthn defines how web applications can access and utilize biometric hardware (including other authentication means) and perform user authentication. WebAuthn was submitted by the Fast Identity Online (FIDO) Alliance, an open industry association that works on authentication standards and was published by W3C. This standard is backed by major corporations such as Google, Paypal, Mozilla, Microsoft, and Qualcomm.

WebAuthn defines a standard web API that can be incorporated into web browsers and related web platform infrastructure. It allows users to use new authentication methods on the web, in the browser and across sites and devices. WebAuthn aims to provide alternatives to password based authentication environment and allows users to use biometric authenticators like voice, fingerprint, USB token, YubiKey, etc. based on public key cryptography.

W3C also announced that major web browsers like Chrome, Edge, and Firefox will soon support signing into online accounts using fingerprint scanners, voice authentication, facial recognition, and so on without the need of any additional software.

How does web authentication work?

Web Authentication works along with other industry standards such as Credential Management Level 1 and FIDO 2.0 Client to Authenticator Protocol 2. A new set of public-key credentials are created by the authenticator during the registration. This new set of public-key credentials can be used to sign a challenge generated by the relying party. The public part of these new credentials, along with the signed challenge, can be sent back to the relying party for storage. The relying party can later use these credentials to verify the identity of a user whenever required.

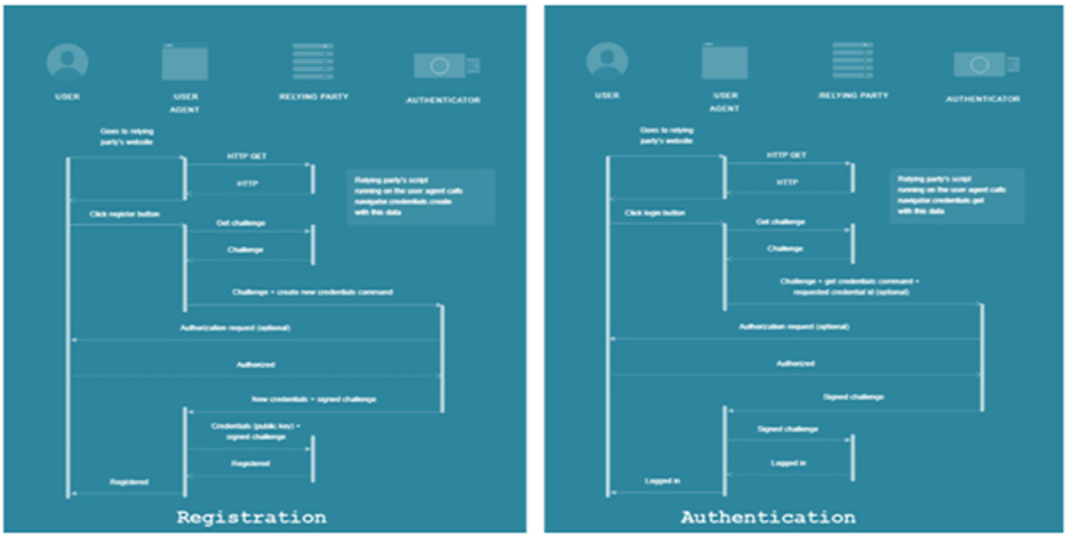

Image: Illustration of registration and authentication with WebAuthn API

The web authentication API has two main methods:

> navigator.credentials.create(): When used with the publicKey option, creates new credentials, either for registering a new account or for associating a new asymmetric key pair credentials with an existing account.

> navigator.credentials.get(): When used with the publicKey option, uses an existing set of credentials to authenticate to a service, either logging a user in or as a form of second-factor authentication.

This method creates new credentials when used with publicKey option. and navigator.credentials.get. There is also an accessory API to list authenticators. The Web Authentication API extends the Credential Management navigator.credentials.create() and navigator.credentials.get()JavaScript methods so they accept a publicKey parameter. The create()method is used for registering public key authenticators as part of associating them with user accounts (possibly at initial account creation time but more likely when adding a new security device to an existing account) while the get() method is used for authenticating (such as when logging in).

Here is a sample call of the create function inside an EJS template:

```
navigator.credentials.create({
publicKey: {
// random, cryptographically secure, at least 16 bytes
challenge: base64url.decode('<%= challenge %>'),
// relying party
rp: {
name: 'Awesome Corp' // sample relying party
},
user: {
id: base64url.decode('<%= id %>'),
name: '<%= name %>',
displayName: '<%= displayName %>'
},
authenticatorSelection: { userVerification: "preferred" },
attestation: 'direct',
pubKeyCredParams: [
{
type: "public-key", alg: -7 // "ES256" IANA COSE Algorithms registry
}
]
}
}).then((res) => {
var json = publicKeyCredentialToJSON(res);
// Send data to relying party's servers
post('/webauthn/register', {
state: '<%= state %>',
provider: '<%= provider %>',
res: JSON.stringify(json)
});
}).catch(console.error);
```

Here is a sample call of the get function in an EJS template:

```
navigator.credentials.get({
publicKey: {
// random, cryptographically secure, at least 16 bytes
```

```
challenge: base64url.decode('<%= challenge %>'),
allowCredentials: [ {
id: base64url.decode('<%= id %>'),
type: 'public-key'
}],
timeout: 15000,
authenticatorSelection: { userVerification: "preferred" },
}
}).then((res) => {
var json = publicKeyCredentialToJSON(res);
// Send data to relying party's servers
post('/webauthn/authenticate', {
state: '<%= state %>',
provider: '<%= provider %>',
res: JSON.stringify(json)
});
}).catch(err => {
alert('Invalid FIDO device');
});
```

If users use Auth0, they don't need to understand all the details of web authentication to use it.

Web-based fingerprint and cloud fingerprint system

We discussed how a web-based fingerprint system allows users to use fingerprints for authentication on web applications and other web-based services. For instance, you can use your fingerprints to access your email account on a browser that offers web-based fingerprint authentication. In this case, your credentials are can be securely stored on the local system, which are used by the web applications to perform a match, when you try to login to your account.

A good analogy for web-based fingerprint can be the use of fingerprints for authentication on mobile phones. On mobile phones with fingerprint sensors, your encrypted fingerprint template is stored locally (i.e. on the mobile phone) and never leaves the device.However, mobile apps can still use your fingerprint to authenticate identity. Each time you login to a mobile app using fingerprint, the app will place a request for match the freshly acquired sample with the stored one.

Now with the inception of cloud computing,things are swiftly moving beyond web-based fingerprint systems.

Cloud computing offers processing power of cloud servers on an ordinary PC or smartphone. Even the tasks, which would have been otherwise impossible to process by a device, can be accomplished with cloud computing. With growing use, new and innovative use cases of cloud computing are emerging.

More and more services and applications are getting on the cloud and biometrics is not an exception. People are increasingly switching to cloud for their personal as well as business computing needs. This trend is evident across all business sizes: small businesses to large enterprises, which are taking up cloud to cut operational as well as maintenance cost of in-house IT applications.

Voter Registration

Windows Biometrics

Workforce Management

Unlike web based fingerprint authentication, in which your biometric credential may reside on the local device and all biometric data processing ability is provided by the local machine, a cloud fingerprint system allow users to authenticate biometrically without setting up biometric capabilities locally. A cloud fingerprint system is an approach in which well-established methodologies of SaaS (Software as a Service) model are leveraged to enable biometric fingerprint recognition over the cloud and offer it as a service.

Unique advantages offered by a cloud fingerprint system

We have discussed advantages of a web based fingerprint system above. A cloud fingerprint system takes web based fingerprint system to the next level and offers several advantages:

- Cloud fingerprint system can be expanded on-demand, more endpoints can be introduced without entangling in technicalities
- Quickly deployment and easy to setup
- Easy to use
- No hassles of buying additional systems
- No need to deploy security for biometric data
- Comparatively cheaper than maintaining in-house locally networked biometric systems

Conclusion

People familiar with web applications available during the early days of this century, know how dramatically they have grown and captured a significant market now. It took some time for web applications to mature but finally here they are. Many web applications are now backed by enormous power of cloud servers, unlike locally installed applications, which are limited to local computational ability. Not only that, they are also backed by large technology corporation. Considering all these factors, web applications are set to even grow even more.

Now is the perfect time that web applications take advantage of biometrics and other authentication methods to eliminate friction and insecurities associated with passwords. Introduction of new standards such as WebAuthn, we may soon start to love forgetting passwords.

ABOUT THE AUTHOR

Danny Thakkar is Senior Product Manager at Bayometric, one of the leading biometric solution providers in the world. He has helped large organizations like Pepsi, America Cares, Michigan State and many other medium and small businesses achieve their identity management needs. He has been in the Biometric Industry for 10+ years and has extensive experience across public and private sector verticals. Currently, he is chief evangelist for Touch N Go and blogs regularly at www.bayometric.com and www.touchngoid.com.

About Bayometric

Bayometric is a leading global provider of biometric security systems offering core fingerprint identification solutions. Learn more

Products We Offer

- Touch N Go
- Single Sign-On
- Biometric Access Control
- Biometric Security Devices
- Fingerprint Scanners
- FBI Certified Readers
- Live Scan Systems
- OEM Modules

Contact Us

Your Name *

Your Business Email *

Your Phone *

SEND

Recent from Blog

Applications of Live Scan Fingerprinting: FDLE, FINR FBI Live Scan

June 22, 2021

Biometric Technologies th Improve Manufacturing S

March 17, 2021

Covid-19 and Security: Wh the Security System Indus like in 2021?

February 4, 2021