On the Security of Authentication when Linking Federated Identities

Bjorn Oude Roelink
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
b.m.ouderoelink@student.utwente.nl

ABSTRACT

Authenticating for an account is increasingly more common for web-based services. This leads to secure and easy authentication methods being more necessary than ever before. For that reason, logins by means of federated identity providers like Google, Facebook, Twitter etc. are becoming a more common authentication method. Services that allow to create an account by using federated identities often also allow creation of a local account. In some cases, these local and federated accounts get linked together. This can have serious security implications for users on websites that perform such linking, such as an attacker gaining access to local user accounts.

This research aims to collect information on how common the practice of linking local and federated identities is and what the security implications of linking those different identities are. To do so, we examine 60 websites that allow a user to log in with both a local and federated identity, and survey whether these identities get linked together and if so in what way. We analyse the results to determine to what degree service providers on the Internet link federated accounts, and what that means for the security of the service and their users.

The contribution of this paper is that it shows that 46 of 60 researched websites link federated logins to a local account. Of those 46 websites 35 do so implicitly, i.e. without notifying the user and asking for authentication for the local account. That shows that there are improvements to be made in using federated identities for authentication.

Keywords

authentication, federated identity provider, identity linking, security, OpenID Connect, SAML

1. INTRODUCTION

Authenticating for an account is increasingly more common for web-based services. This leads to secure and easy authentication methods being more necessary than ever before. An increasingly more common authentication method for that reason is using federated identity providers. Examples of such identity providers are Google [1], Facebook [2] and Twitter [3]. Users might be familiar with this authentication method in the form of a ”Login with ...” or ”Continue with ...” button. Most web services that allow the use of federated identity providers also allow a user to make a local account. When a user already has a local account and tries to log in using a federated identity, that service might choose to link these authentication methods and log the user into the existing local account. That practice poses security concerns, especially when the website does not ask the user to authenticate to the local account before establishing this link. The reason of concern is that an attacker can now also access these local accounts when they obtain access to an account usable as federated identity. The attacker can subsequently steal private data and lock the owner out of their account.

The goal of this research therefore is to examine how common it is for services to link together local and federated identities and what the security implications of that are. We aim to give recommendations on improving the security of using federated identities for authentication. To realize this, we will focus on the usage of federated identity providers at websites that also allow a user to create a local account, and research whether these websites link federated identities to a local account. Based on the results of the research we will form recommendations for users and services on how to safely use federated identity providers for authentication. To form an outcome from the gathered results, we have established the following main research question:

- Do service providers, and if so to what degree, link local and federated identities, and what does this mean for security?

To answer that main research question, we will answer the following sub-questions:

- What fraction of researched service providers link local and federated identities? Can different categories be defined for these service providers?
- What security concerns should be considered when linking identities from different identity providers? To what extent are these considerations currently practised?

The remainder of this paper is organized as follows: First, we provide some background information on federated identities, identity providers and how both work in Section 2. In that section, we also discuss some related works. Then we will cover the methodology of this research in Section 3. We report the results gained from the research in Section 4 and discuss those results and their implications to give recommendations accordingly in Section 5. Section 6 describes the conclusion of this research and mentions possible future work.

33rd Twente Student Conference on IT July 3rd, 2020, Enschede, The Netherlands.

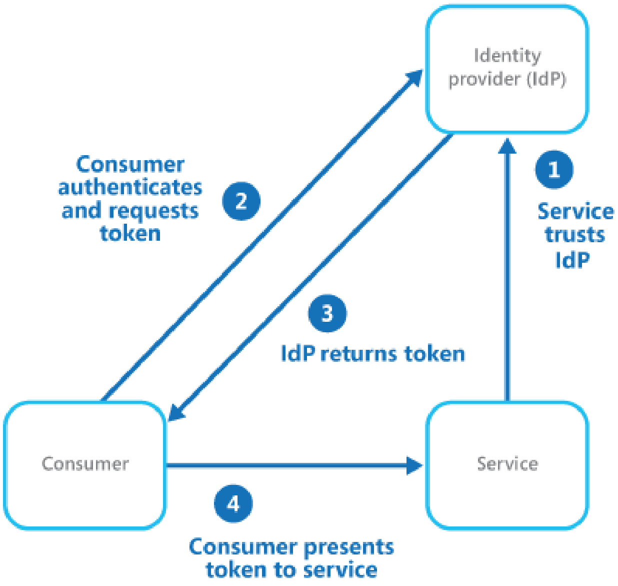


Figure 1. General federated identity pattern. (edited from original) [7]

2. BACKGROUND

Federated identities are identities provided by an external identity provider (IdP). They can be used by a service provider (SP) to let users authenticate to their service.

There are different standards that can be used by IdPs to implement federated identities. The two arguably most used ones are SAML [4] and OpenID Connect [5]. OpenID Connect is built on top of OAuth 2.0 [6] and purpose built for authentication, while OAuth 2.0 itself is more general for authorization and delegation.

What the exact federated authentication flow looks like depends on the standard implemented by the IdP. The general federated identity pattern however proceeds as in Figure 1: For a user to be able to authenticate with a federated identity, the SP first must trust that IdP and allow logins with these identities (step 1). When a user then wants to log in using an IdP, they request a token from that provider (step 2). If that user is not yet authenticated to that IdP then the user will be asked to authenticate themselves to the IdP. The IdP will then return a token (step 3) which should be presented to the SP (step 4). This token represents the user being authenticated and must be verified by the SP with the IdP.

While the token is meant as a proof of authentication, it also allows access to some information on the identity used to log in. The user information retrievable with the token differs for each IdP, but generally includes a name and email address. The fact that the token allows access to some basic user information means that it is possible, for services that allow multiple ways to authenticate, to use attributes of these identities such as the provided email address in order to link the federated identity with an existing local account. In that way these services allow a user access to a common account independent of how they choose to authenticate. In that process, it is however critical that the local account and the account used as federated identity are controlled by the same person to prevent unauthorized access.

2.1 Related Work

All related works we will outline here are not necessarily related to linking of federated identities, but more so focus on the security of using federated identities for authentication. Security of federated identities for authentication is the central focus of this research, and there is an abundance of other papers that apply that same focus to topics different from the one in this research.

The first related work is that by Ghasemisharif et al. [8] in which they describe the security impact a compromised federated identity account can have. They continue with several novel attacks using federated identities and subsequently explore and propose a unified way to revoke access to accounts associated with a federated identity which they call ”Single Sign-Off”. For their research, Ghasemisharif et al. have also created a data set recording federated identity providers available on websites listed in the Alexa top 1,000,000 [9].

Another related work is a research by Fett et al. [10] in which they perform an in-depth security analysis on OpenID Connect which they claim had not been performed yet. To do so, Fett et al. developed a formal model which they use to show that OpenID Connect does fulfill the stated central security properties. In their paper they also describe known and novel attacks on OpenID Connect, and propose security measures on those as guidelines to follow for IdPs implementing OpenID Connect.

A third related work is by Mainka et al. [11]. In their paper the authors describe ways in which attackers can create malicious IdPs in order to compromise accounts on a service. They describe and research three attacks on OpenID Connect called ID Spoofing, Key Confusion and Token Recipient Confusion. In their report they also evaluate whether the vulnerabilities they reported have been resolved. Of the 70 investigated websites, 18 were still vulnerable to at least one of the three reported attacks after one year.

These related works show that there are a lot of different topics for research on the security of federated identity providers and the protocols they implement. Our research in that regard is novel as it researches security aspects of linking federated identities by websites. The results of this research and the corresponding recommendations we will propose will complement the guidelines presented in those related works.

3. METHODOLOGY

3.1 Tooling

We have used the following tools during our research in order to gather the required data:

- Firefox Developer Edition
- ProtonMail
- ProtonVPN
- Phone with a prepaid phone number

Firefox is chosen as the browser for its many privacy settings and good support across the Internet. ProtonMail is chosen as email provider to create an email address which was used for all subsequently made accounts. The reason ProtonMail is chosen is because an account at this email provider cannot be used as a federated identity, which would be the case for Gmail (Google), Yahoo! Mail (Yahoo), Outlook (Microsoft), etc. This makes sure that no federated identity must be ruled out because it is also the email provider and might therefore be treated differently. The created ProtonMail account can also be used to access the ProtonVPN service. The reason for using a virtual private network (VPN) during the research is to prevent an account from being linked or banned on the basis of an IP address or other attributes of a connection that the account has in common with accounts that are not researched, such as our personal accounts. A phone in combination with a prepaid phone number is used to create accounts that require a telephone number for verification purposes, e.g. Google.

3.2 Input Data

For the websites to research, we intended to use a data set provided by the research by Ghasemisharif et al. [8] as mentioned in Section 2.1. Many websites in this data set however appeared to be outdated already, i.e. the identity providers that can be used on a website according to the data set did not always correspond to reality anymore. Other sites on the list could not be researched because of a language barrier. As such we created a custom list of websites to research using the data set as starting point. For each site in the data set that was usable, we added well known sites with similar functionality that also allowed federated logins. The list we created consisted of 88 websites, and the identity providers used most would be examined in our research. These IdPs would have been Facebook (64 sites), Google (61 sites), Apple (19 sites), Twitter (12 sites) and Yahoo (7 sites). These five identity providers together would have covered 85 websites, as listed in Table 2 included as an appendix in Section 8. However, due to only using a pseudonym identity in this research and Facebook requiring a picture of a real person upon account creation, Facebook could not be included as an IdP in this research. Similarly, creating an Apple account was possible, however using this account for federated logins requires an Apple device. As no such device is available for this research, Apple will not be included as an IdP in this research either. Excluding websites that would not function properly during research, the three remaining identity providers cover 60 websites which we use as input data for the research.

3.3 Measurements

The first thing we did before taking any measurements is to connect the VPN for reasons described in Section 3.1. For each website, we perform the steps in Figure 2. First, we register a local account at the current website (step 1). Then, we need to find a way to recognize this account. To do so, we find or create an identifier (step 2). Sometimes this identifier is a literal account ID code in the settings, for other websites we create this identifier by adding a specific thing to a favourites list, etc. Then the browser is cleared to make sure that no login information of the local account remains (step 3). After that, we log in on the website using a federated identity (step 4) and document the results of this login (step 5). If authenticating to the federated identity logs us into an account immediately, we verify whether this is the local account by examining the presence of the identifier from step 2. Then we clear the browser again to make sure no login information remains. Steps 4-6 will be repeated for every federated identity provider in this research that is available for authentication. This process is then repeated for all websites in this research as described in Section 3.2.

4. RESULTS

The result of performing the measurements as described in Section 3.3 for all three identity providers on all websites in this research gave the results as listed in Table 1.

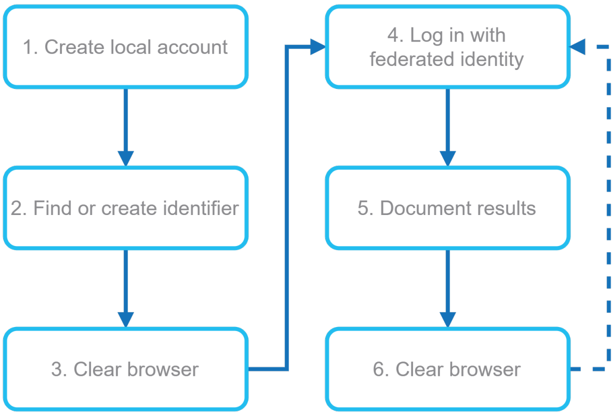


Figure 2. Per website measurement process

Table 1 shows which sites have been researched and the federated identity providers that were available. An open circle denotes that the IdP is available for authentication on that website. A filled circle means that the website allows an IdP for authentication and links the federated identity to a local account. Whether the website does so explicitly and only after authenticating for the local account or implicitly without authentication to the local account, is indicated with a check mark or exclamation point respectively inside the filled circle.

Of the 60 researched websites, 46 (77%) link federated identities to local accounts for at least one of the available identity providers. Regarding the 46 websites that perform this practice, only 12 of them ask the user to authenticate the local account before the federated identity is linked. The other 34 websites do this linking implicitly and consequently allow access to the local account while the user has not proven that they had control over the local account. Only 14 websites do not link any federated identity to local accounts.

An example of a website that does well is jottacloud.com. This website explains to the user that the Google account used as federated identity has not been used before. The user is then given the option to create a new account or link it with the existing local account. Upon choosing the option to link the account, the user needs to authenticate to that local account in order to establish the link. This process can also be seen in Figure 3. So, the user is given the explicit option to link identities but must authenticate to all identities involved to do so.

In that same category, box.com does not do well. Upon logging in with Google, the user is immediately given full access to the local account without any form of authentication. The local and federated identities have been linked in a non-explicit way without the user needing to authenticate for the local account.

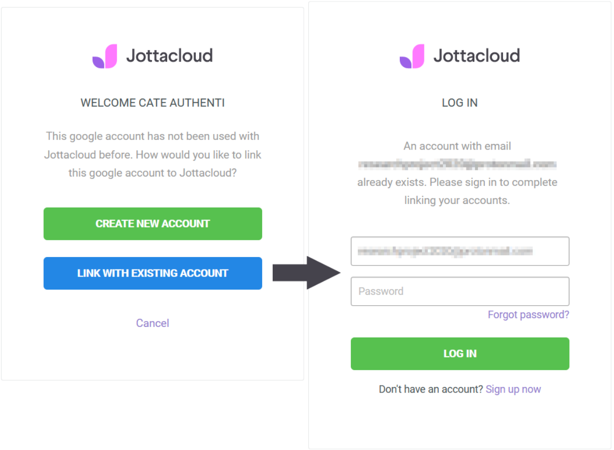
We will discuss what the security implications of these results are in Section 5.1.

5. DISCUSSION

As discussed in Section 3.2, Facebook and Apple have not been incorporated as identity providers in this research for reasons described in that section. Does that, excluding the number 1 and 3 of the top 5 of identity providers for the examined websites, pose a problem for the validity of this research? Even taking the importance of these identity

		Logins		
Website	Category	G	🐦	Y
adfly.com	advertisements	❗		
getpocket.com	application	❗		
thefreedictionary.com	application	❗	○	○
4shared.com	cloudstorage	○	○	
box.com	cloudstorage	○		
degoo.com	cloudstorage	○		
dropbox.com	cloudstorage	❗		
idrive.com	cloudstorage	○		
jottacloud.com	cloudstorage	✔		
jumpshare.com	cloudstorage	❗		
koofr.eu	cloudstorage	❗		
mediafire.com	cloudstorage		○	
pcloud.com	cloudstorage	❗		
rapidgator.net	cloudstorage	❗		
zoolz.com	cloudstorage	○		
taringa.net	entertainment	❗		
9gag.com	entertainment	❗		
battle.net	entertainment	✔		
deezer.com	entertainment	❗		
epicgames.com	entertainment	✔		
fandom.com	entertainment	○		
imdb.com	entertainment	✔		
imgur.com	entertainment	❗	○	○
nicovideo.jp	entertainment	○	○	○
scribd.com	entertainment	❗		
soundcloud.com	entertainment	❗		
tidal.com	entertainment		❗	
tunein.com	entertainment	❗		
vimeo.com	entertainment	○		
stackoverflow.com	forum	❗		
xda-developers.com	forum	○		
patreon.com	fundraiser	❗		
buzzfeed.com	news	○		
dailymail.co.uk	news	❗	○	
marketwatch.com	news	✔		
medium.com	news	❗	❗	
nytimes.com	news	❗		
techcrunch.com	news			✔
theverge.com	news	○	○	○
asana.com	productivity	❗		
canva.com	productivity	✔		
gitlab.com	productivity	○	○	
trello.com	productivity	✔		
zoom.us	productivity	❗		
etsy.com	retail	❗		
rakuten.com	retail	❗		
asus.com	retail	❗		
dell.com	retail	❗		
adidas.com	retail	❗		❗
asics.com	retail	✔		
reebok.com	retail			❗
avast.com	security	❗		
avira.com	security	❗		
malwarebytes.com	security	❗		
airbnb.com	services	✔		
booking.com	services	✔		
fiverr.com	services	✔		
hubspot.com	services	❗		
realtor.com	services	❗		
uber.com	services	○		

Table 1. Linking of federated logins by websites.
○: login available; no linking possible
❗: login available; linked implicitly
✔: login available; linked explicitly with password



Jottacloud

WELCOME CATE AUTHENTI

This google account has not been used with Jottacloud before. How would you like to link this google account to Jottacloud?

CREATE NEW ACCOUNT

LINK WITH EXISTING ACCOUNT

Cancel

Jottacloud

LOG IN

An account with email [redacted] already exists. Please sign in to complete linking your accounts.

[redacted]

Password

Forgot password?

LOG IN

Don't have an account? Sign up now

Figure 3. Jottacloud login with Google

providers in mind, the results of this research would not be substantially different. Websites would still be found to implicitly link federated identities to local accounts if they did so during this research. The only possibility in adding more federated identity providers is for the security implications to be pose a bigger or smaller risk. As such it would not have an impact on the recommendations in Section 5.2, nor on the conclusion in Section 6 as the implications for security are the same. The biggest impact in excluding two of the largest identity providers is that currently no data is known on which website apply linking with these IdPs and whether they do so explicitly or not. This might be interesting information to research for comparison and improvement reasons and will as such be mentioned in Section 6.1 on future work.

5.1 Security Implications

Now to discuss the results gathered during this research: what are their implications for security? Based on the gathered results, there are quite some security implications that this research uncovers. These implications are best discussed by first making an attacker model.

5.1.1 Attacker Model

What reasons might an attacker try to gain access to an account for, and how could this be organized? The most obvious answer to the first question is money, information or both. One might already start to see why sites in certain categories listed in Table 1 are therefore a target. It seems most likely that an attacker will focus on the cloud storage and productivity categories if they want to gather potentially secret information. Other categories that might be of interest for an attacker because of the payment information such as credit cards that might be linked to them are entertainment, retail, security and services. One last area of focus is the fundraiser category for the money that flows through accounts on platforms in that category.

To try and log into an account, an attacker will always want to find the weakest link that gives the most opportunities. Federated logins, especially those that can be used on many services, are therefore striking targets for attackers. This research has shown already that more than half of the researched websites give access to a local account by logging in with a federated identity with the same mail address, even if performed for the first time. When this federated identity is then also badly secured, as might be the case for old and abandoned accounts which have not been used in a long time, this might combine to a highly undesirable situation. The password for such an abandoned account might not have been updated for years and could have been leaked. The risk of passwords leaking out is especially large when they have been reused on other websites [12]. When an attacker gains access to an account that can be used as a federated identity, they can gain access to all local accounts on sites that links these together without authentication for the local account. Obtaining access to not one but multiple accounts at the same time increases the damage that can be caused.

5.1.2 Risks

There are three main risks that that come with hijacked account which we will discuss in this section. We will describe them as separate, but these co-occur and the boundary between them is rather blurred. The three risks are theft, impersonation and fraud, and they are not only relevant for the owner of an account.

Theft is the risk that an attacker takes something that does not belong to them. This risk is most prevalent for the cloud storage and fundraiser categories. Cloud storage is used by consumers to store files which can include sensitive information such as banking details, medical papers or family photos with high emotional value. When an account at a cloud storage provider is taken over, the personal data stored there can be stolen by the attacker. For fundraisers, the risk of theft lies therein that when an attacker manages to gain access when a fundraiser is ongoing, then they might be able to route the payout of that fundraiser to them instead of the account owner.

Impersonation is when the hijacker of an account pretends to be the owner of that account. This risk is most prevalent for the entertainment, news and productivity categories. When an attacker obtains access to an account in such category, they can misuse this account to make others believe false information. This can severely damage the reputation of the owner. When the impersonator misuses the trust that other people have in the owner of the account is when this risk blends into the next.

Fraud is when someone uses intentional deception for unlawful gain. The risk for hacked accounts is that the attacker uses them to sell goods or services which they receive the money for after which the attacker disappears. Stolen Amazon accounts for example are used to sell items which never end up being delivered to the buyer [13]. This risk is not contained to the owner of the account and has a serious monetary effect to people who purchased products from the fraudulent seller. At the same time, the fraud can cause the original owner whose personal information is linked to the exploited account to get into serious trouble with the law. Worst case, they might be sentenced to jail for frauds they did not perform.

5.2 Recommendations

The recommendations given in this section stem from the results of this research listed in section 4, and the corresponding discussion in section 5 above.

For websites, or more generally services, we recommend to

1. only ever explicitly link federated identities to local identities. Ask for authentication to the local account before doing so.
2. keep in mind the security implications of adding more federated identities, and which login method might be the weakest link.

For users, our recommendations are to

1. keep all accounts secure, even when not using them. This is especially important for accounts that can be used as a federated identity. A good option is to delete accounts that will not be used in the foreseeable future.
2. enable two-factor authentication (2FA) for accounts usable as federated identity. For local accounts it is currently unknown whether enabling 2FA helps against implicit linking of federated identities.

These recommendations will go a long way to diminish the risks caused by websites that link federated identities to local accounts as uncovered by us in this research.

6. CONCLUSION

The data resulting from this research uncovers that more than 75% of the researched websites link federated identities for authentication. Using this data, we will answer the different research questions, starting with the subquestions.

> What fraction of researched service providers link local and federated identities? Can different categories be defined for these service providers?

From the results in Section 4 we can conclude that 46 of 60 researched sites link at least one of the federated identities available for authentication to local accounts. Of those 46, only 12 do so explicitly by asking the user to authenticate the local account. The other 34 websites do not ask for authentication and implicitly link the federated identity. We see no indication that websites in certain categories do link federated identities to local accounts while websites in other categories do not. No conclusive statements on that can be made however, as not all possible categories are represented in this research, and we have not selected the researched websites specifically for their categories.

> What security concerns should be considered when linking identities from different identity providers? To what extent are these considerations currently practised?

The main security consideration when linking identities from different identity providers is to not trust that two identities are controlled by the same person until proven. This means that if it is possible to link multiple identities, then all the identities involved should be authenticated in order to do so. As we discovered during this research, less than 50% of the researched websites practice this. Another security concern to consider is that having multiple methods to authenticate increases the attack surface of that account. The complementary security aspect to this is that of the weakest link, where an attacker can now choose the weakest point to gain access to that account. This is especially important when using a federated identity provider allows circumventing two-factor authentication (2FA) on another method to log in. Since 2FA is not in the scope of this research, these considerations will be discussed as future research in Section 6.1

Using the answers to the sub-questions above, we will answer the main research question.

> Do service providers, and if so to what degree, link local and federated identities, and what does this mean for security?

During this research we established that service providers do in fact link local and federated identities. 34 of the researched websites that allow users to log in using federated identities, link those identities to local accounts in a way that imposes big security risks. For these different login methods to be linked, the user does not have to authenticate to the local account in order to establish the link. While this may be convenient for the user, this is unwanted behaviour and this practice poses big security risks as described in Section 5.1.2. Whenever an attacker gains access to an account usable for federated logins, they can also access local accounts, and their associated data, on services that implicitly link logins for this federated login provider. This allows an attacker to gain access to all information stored on that local account, lock a user out of their own account and abuse the account for all sorts of criminal purposes. For this reason, there are improvements to be made by these services in their use of federated identity providers as recommended in Section 5.2, of which the most important is that services should ask a user to authenticate to the local account before the federated identity is linked.

6.1 Future Work

With the limitations and results of this research come quite some opportunities for future research. The obvious one would be a continuation of this research which would include Facebook and Apple as identity providers. The inclusion of Facebook in a future research would mainly be interesting because, at least for the list of websites originally accumulated for this research, Facebook is the federated identity provider supported on most sites. Therefore, it would be interesting to see whether the most prevalent provider is a paragon for other identity providers, or whether websites implemented it in the same way they have implemented other identity providers. The same applies to Apple, as the third largest identity provider in the original accumulated list of websites. Something that would be interesting specifically for Apple is that it apparently needs an Apple device in order to be used as an identity provider. Whether this functions as some sort of two-factor authentication (2FA), and what this would mean in the context of this research, would have to be studied.

2FA is also an integral part in another possible future research, namely on what impact enabling 2FA on local accounts would have on the results gathered in this research. In this research we have not looked at the effect of that on linking these identities to local accounts and what this means for subsequent logins. This can be an interesting research as using federated identity providers might be a way for attackers to circumvent 2FA and thereby being able to take over an account when the user thinks he or she is protected by 2FA. Research on this topic could propose a method to discover which login is the ”weakest link”.

7. REFERENCES

[1] Google, “Integrating Google Sign-In into your web app,” May 2020. [Online]. Available: https://developers.google.com/identity/sign-in/web/sign-in

[2] Facebook, “Facebook Login - Documentation,” Jul. 2018. [Online]. Available: https://developers.facebook.com/docs/facebook-login

[3] Twitter, “Log in with Twitter,” Jun. 2020. [Online]. Available: https://developer.twitter.com/en/docs/basics /authentication/guides/log-in-with-twitter

[4] Oasis, “SAML Version 2.0 Errata 05,” May 2012. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.html

[5] OpenID, “OpenID Connect | OpenID,” Aug. 2018. [Online]. Available: https://openid.net/connect

[6] OAuth, “OAuth 2.0 — OAuth,” Jun. 2020. [Online]. Available: https://oauth.net/2

[7] Microsoft, “Federated Identity pattern - Cloud Design Patterns,” Jun. 2017. [Online]. Available: https://docs.microsoft.com/en-us/azure/architecture/patterns/federated-identity

[8] M. Ghasemisharif, A. Ramesh, S. Checkoway, C. Kanich, and J. Polakis, “O Single Sign-Off, Where Art Thou? An Empirical Analysis of Single Sign-On Account Hijacking and Session Management on the Web,” in *27th USENIX Security Symposium*, Aug. 2018, p. 19. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/ presentation/ghasemisharif

[9] Alexa, “Alexa - Top sites,” Jun. 2020. [Online]. Available: https://www.alexa.com/topsites

[10] D. Fett, R. Küsters, and G. Schmitz, “The Web SSO Standard OpenID Connect: In-depth Formal Security Analysis and Security Guidelines,” in *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, Aug. 2017, pp. 189–202.

[11] C. Mainka, V. Mladenov, and J. Schwenk, “Do Not Trust Me: Using Malicious IdPs for Analyzing and Attacking Single Sign-on,” in *2016 IEEE European Symposium on Security and Privacy (EuroS P)*, Mar. 2016, pp. 321–336.

[12] T. Hunt, “The only secure password is the one you can’t remember,” Mar. 2011. [Online]. Available: https://www.troyhunt.com/only-secure-password-is-one-you-cant

[13] B. Krebs, “amazon hacked seller account — Krebs on Security,” Apr. 2017, library Catalog: krebsonsecurity.com. [Online]. Available: https://krebsonsecurity.com/tag/amazon-hacked-seller-account

8. APPENDICES

Website	Category	Local	f	G		🐦	Y
adfly.com	advertisements	○		○			
taboola.com	advertisements	○		○			
getpocket.com	application	○		○	○		
thefreedictionary.com	application	○	○	○		○	○
4shared.com	cloudstorage	○	○	○		○	
box.com	cloudstorage	○		○			
degoo.com	cloudstorage	○		○			
dropbox.com	cloudstorage	○		○			
idrive.com	cloudstorage	○		○			
jottacloud.com	cloudstorage	○	○	○			
jumpshare.com	cloudstorage	○		○			
koofr.eu	cloudstorage	○		○			
mediafire.com	cloudstorage	○				○	
pcloud.com	cloudstorage	○	○	○	○		
rapidgator.net	cloudstorage	○	○	○			
zoolz.com	cloudstorage	○	○	○			
naver.com	combination	○	○				
taringa.net	combination	○	○	○			
9gag.com	entertainment	○	○	○			
battle.net	entertainment	○	○	○	○		
deezer.com	entertainment	○	○	○			
epicgames.com	entertainment	○	○	○			
fandom.com	entertainment	○	○	○			
gfycat.com	entertainment	○	○				
giphy.com	entertainment	○	○		○		
hatena.ne.jp	entertainment	○		○			
imdb.com	entertainment	○	○	○	○		
imgur.com	entertainment	○	○	○		○	○
nicovideo.jp	entertainment	○	○	○	○	○	○
roblox.com	entertainment	○	○				
scribd.com	entertainment	○	○	○			
soundcloud.com	entertainment	○	○	○	○		
spotify.com	entertainment	○	○		○		
tidal.com	entertainment	○	○		○	○	
tunein.com	entertainment	○	○	○	○		
twitch.tv	entertainment	○	○				
vimeo.com	entertainment	○		○			
stackoverflow.com	forum	○	○	○			
xda-developers.com	forum	○		○			
fundly.com	fundraiser	○	○			○	
gofundme.com	fundraiser	○	○				
indiegogo.com	fundraiser	○	○				
kickstarter.com	fundraiser	○	○				
patreon.com	fundraiser	○	○	○			
blastingnews.com	news	○	○	○			
buzzfeed.com	news	○	○	○	○		
cnet.com	news	○	○				
dailymail.co.uk	news	○	○	○		○	
engadget.com	news	○	○				
fantasypros.com	news	○	○				
marketwatch.com	news	○	○	○			
medium.com	news	○	○	○	○	○	
nytimes.com	news	○	○	○	○		
sky.com	news	○					○
techcrunch.com	news	○					○
theverge.com	news	○	○	○		○	○
welt.de	news	○	○				
wired.com	news	○		○			
zdnet.com	news	○	○				
asana.com	productivity	○		○			
canva.com	productivity	○	○	○			
gitlab.com	productivity	○		○		○	
trello.com	productivity	○		○			
zoom.us	productivity	○	○	○			
buyma.us	retail	○	○				
etsy.com	retail	○	○	○	○		
rakuten.com	retail	○	○	○	○		
acer.com	retail	○	○	○		○	
asus.com	retail	○	○	○			
dell.com	retail	○	○	○			
adidas.com	retail	○		○			○
asics.com	retail	○	○	○	○		
reebok.com	retail	○	○				○
underarmour.com	retail	○	○				
avast.com	security	○	○	○			
avira.com	security	○	○	○			
kaspersky.com	security	○	○				
malwarebytes.com	security	○	○	○			
airbnb.com	services	○	○	○	○		
booking.com	services	○	○	○	○		
fiverr.com	services	○	○	○	○		
hubspot.com	services	○		○			
realtor.com	services	○	○	○			
tinder.com	services	○	○				
uber.com	services	○	○	○			

Table 2. Initial list of websites and identity providers