Cloud Computing Security

Users authentication

**Timothy FABELURIN**

2022

# ABSTRACT

Cloud computing is a developing of area of technology which is receiving acceptance by the public at a high rate. The swift acceptance and advancement in the technology, bring about a lot of security risk and variety of vulnerabilities that are being exploited by malicious users to gain access stored data in cloud environment. Since access to the cloud resource is required for attacker, this makes it a critical aspect for both cyber security experts to secure and attackers to exploit. This report analyze different authentication methods in cloud and focus more on the loophole with the use of application access tokens as a means of authorization and authentication.

***Keywords: Cloud Computing, Authentication, OAuth protocol, SAML Protocol, User credentials, cybersecurity.***

Contents

[ABSTRACT 1](#_Toc98525308)

[1.0 INTRODUCTION 4](#_Toc98525309)

[1.1 History of Cloud Computing 4](#_Toc98525310)

[1.2 The revolution of Cloud computing 4](#_Toc98525311)

[1.3 Service Delivery models 5](#_Toc98525312)

[1.3.1 Software as a Service: 5](#_Toc98525313)

[1.3.2 Platform as a Service 5](#_Toc98525314)

[1.3.3 Infrastructure as a Service 5](#_Toc98525315)

[1.4 Deployment Model 5](#_Toc98525316)

[1.4.1 Public cloud 5](#_Toc98525317)

[1.4.2 Private cloud 6](#_Toc98525318)

[1.4.3 Community cloud 6](#_Toc98525319)

[1.4.4 Hybrid cloud 6](#_Toc98525320)

[2.0 BACKGROUND OF CLOUD SECURITY 6](#_Toc98525321)

[2.1 Contextualization 6](#_Toc98525322)

[2.2 Cloud Security Alliance (CSA) 7](#_Toc98525323)

[2.3 Cloud Security Framework 8](#_Toc98525324)

[2.4 NIST Guidelines on Cloud Security and Privacy Issues and Recommendations 8](#_Toc98525325)

[3.0 SECURITY RISK IN CLOUD AUTHENTICATION 10](#_Toc98525326)

[3.1 Multi-factor Authentication 10](#_Toc98525327)

[3.2 SAML Authentication 10](#_Toc98525328)

[3.3 OAuth 11](#_Toc98525329)

[3.4 OpenID 12](#_Toc98525330)

[3.5 Security Risk involves in Using Access tokens for Authorization and authentication 12](#_Toc98525331)

[4.0 CASE STUDY 14](#_Toc98525332)

[4.1 Pawn Storm attacks against the Democratic National Convention (DNC) 14](#_Toc98525333)

[4.1.1 Procedure of used to abuse OAuth 14](#_Toc98525334)

[4.2 SolarWinds backdoor used in Nation-State Cyber Attacks 17](#_Toc98525335)

[4.2.1 Long Term Access 18](#_Toc98525336)

[5.0 COUNTERMEASURES AGAINST THE RISKS 18](#_Toc98525337)

[5.1 Restriction of Web-based Content 18](#_Toc98525338)

[5.1.1 Configuring User consent setting on Azure 19](#_Toc98525339)

[5.1.2 Prevent Users from Registering new applications 19](#_Toc98525340)

[5.2 User Training 20](#_Toc98525341)

[5.3 Setup Automated Response 20](#_Toc98525342)

[Sign-in risk policy 20](#_Toc98525343)

[6.0 CONCLUSION 23](#_Toc98525344)

[8.0 References 24](#_Toc98525345)

# 1.0 INTRODUCTION

The revolution is happening with the media in term of decentralized information and easy of accessibility of new is also being experienced in the IT industry with respect to Cloud computing. Private owned applications are now hosted on a public shared infrastructure being managed by third party without little or no control of the base infrastructure, security etc. Not just the software applications but almost all (if not all) IT resources can now be hosted hundreds or thousands of miles away entrusted to a service provider while organizations focus on other business needs. The extent at which cloud computing is being globally accepted now would have been unimaginable some years back.

## 1.1 History of Cloud Computing

Cloud computing is the concept by which an environment that comprising of IT resources and services are created on a shared platform and being made available for users to deploy and consume the services via internet. The IT resources includes hardware, Network, software, and other associated services. This can easily be imagined to be like an electricity grid but in this case for computers where shared resources, information and software are provided to users on-demand. The explanation of “cloud computing” from the National Institute of Standards and Technology (NIST) (P.Mell and T. Grance, 2009.) is that “cloud computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”.

## 1.2 The revolution of Cloud computing

The concept of cloud computing was suggested by John McCarthy first time ever in 1960s. He stated that calculations would be carried out in the future public utilities. However, the idea of cloud computing only became popular in 2007 and in 2008, it became subjects of discuss in conferences. The term cloud was first used by Eric Schmidt who was head of Google, and thereafter publicized by the media.

There seem to be different opinion among technology historian on how cloud computing came to be and the main technologies that led to this paradigm, however, many believes that virtualization and increase of bandwidth of internet connectivity largely contributed to this thought of providing service on a rental scheme.

Due to the cloud computing, Government IT operations has been revolutionized “Governments are now leveraging the cloud for its flexibility, operational benefits, and substantial cost savings. For example, in May 2009, the Japanese government announced the Kasumigaseki Cloud; in September 2009, the US government launched the Cloud Computing Mall; and in January 2010, the UK government introduced the G-Cloud government cloud infrastructure. Successful businesses— which are currently migrating services to the cloud and relying on it to help manage hardware and software—will soon have no headquarters or IT infrastructure.” (Irena Bojanova, 2013)

Also, because of the advancement made in cloud computing and due to several IT related complexities, businesses of all sizes have swiftly plugged into the acceptance of the technology. The related issue includes constant rise in IT cost, energy demands and expenses, server spawl, scalability, maintenance and support and required talents to manage infrastructure and services, Time to market pressure, among other factors.

## 1.3 Service Delivery models

There are three main models in which cloud computing service can be rendered. They are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

### 1.3.1 Software as a Service:

In this model, licensed software applications are provided by the cloud service provider, giving users the right to have assess to the software and utilizes the functions as a web-based service. Using this model, users are shielded from all the activities that relates to the installation and maintenance of the software and the subscription cost is usually less expensive compared to buying the license in full. Example of SaaS provided is Salesforce, Microsoft O365

### 1.3.2 Platform as a Service

The PaaS gives the capability to the user to deploy applications and solutions on a provided infrastructure. The provider makes available the web servers, databases, programing language execution environment and the operating system software. Example of the PaaS provided are AWS, Azure etc.

### 1.3.3 Infrastructure as a Service

For PaaS model, hardware such as servers, storage, network, and other networking modules are provided by the provided for customer’s consumption. Users is required to installed and maintain all software and applications they required on the provided infrastructure.

## 1.4 Deployment Model

There are mainly four types of cloud. These are, public cloud, private cloud, hybrid cloud and community cloud.

1.4.1 Public cloud**:** A cloud is said to be public cloud when the resources such as, network, servers, applications etc. are provided over a public network and anyone can access it. Security of the is lesser compared to the other clouds.

1.4.2 Private cloud**:** This is an infrastructure that provide service to only one organization. It can be internally managed or by a third party and therefore has less security concerns.

1.4.3 Community cloud**:** this refers to a setup where the infrastructure is shared between organizations within a community that has common goal.

1.4.4 Hybrid cloud**:** is the combination of both private cloud and public cloud and it provides a secure access control to distinct the users.

# 2.0 BACKGROUND OF CLOUD SECURITY

## 2.1 Contextualization

There have been several papers on the hot topic of cloud computing security and privacy, however, most of referenced work either focus the generalized issue on the deployment models or security issue that relates to the service models and slightly discuss on the specific key security issues in cloud computing.

(Rajani Sharma, 2014) discussed how security issues such as Data Confidentiality, Data Availability, Integrity, and trust relates to cloud computing. Providing scenarios and possible solutions. The solutions seem to focus mail on what is required for the cloud service provider (CSP) is to do on their part with little or no mention about user’s responsibilities with respect to security.

(Liliana F. B. Soares, 2013) paper specifically described on securing users authentication in cloud management interface using MFA on the proxy gateway that is shielding the internal network. However, the Paper did not show how this approach will withstand attacks.

The review paper by (Riddhi Doshi, 2020) summarizes security concerns in as related to clous computing and describes some proposed security models like Security access control model, Enhanced Data security model and so on, but it lacks depth of how these models can be applied to tackle the raised security concerns.

(SUN, 2019) discussed solutions to privacy protection techniques in the paper. Various ABE models, and analysis of the integration trend of access control, encryption, trust, and other technologies to achieve better privacy protection where summarized. Current challenges and future directions were provided.

(Michael Kretzschmar, 2011) discussed the Security Management Areas in the Inter-Cloud like the Identity management, credential management, Attribute management, etc. The focus was on following the key managements policies is discussing security solutions for cloud computing but no scenario and methods of applying the procedures was provided.

(Ms.Neha Mahakalkar, 2017) showed the Implementation of Re-encryption Based Security Mechanism to Authenticate Shared Access in Cloud Computing but only gave technical procedure and comparison and analysis carried out with any other methods.

## 2.2 Cloud Security Alliance (CSA)

Security controls in cloud computing is generally like that of anu IT environment. Although some risks are specifically associated to cloud environment due to its operation model used to enable cloud services. The Cloud Security Alliance (CSA) enumerated the following cloud specific security threats (Williams Starllings, 2015):

1. **Insecure interfaces and APIs**

For customer to effectively interact with cloud services, cloud providers expose some software interfaces or APIs. The availability and security of cloud services depends on the basic APIs security. It is important for the interfaces to be designed to protect against attempts of malicious or accidental alteration of the policy regarding the authentication, access control, encryption and activity monitoring.

1. **Malicious insiders**

As enterprise organization relinquishes a lot of control to the cloud service provider. One of the threats to this paradigm is a malicious internal activity within the Cloud provider. Transparency, breach notification, legal contract binding the client and the CP are some measures to counter this type of high risk.

1. **Data leakage or loss**

This is perhaps most devastating for most customers. There are several ways by which data can be compromised. However, an obvious example is the deletion or alteration of records that has no backup of the original content. It is therefore important that unauthorized individual do not gain access to sensitive data

1. **Shared technology issues**

One of the characteristics of Infrastructure-as-a-service vendor is sharing the infrastructure to deliver a scalable service. Unfortunately, the underlying components were not built for proper isolation for multi-tenant architecture even if virtual machine is used for each client. This creates vulnerability by attackers within the cloud environment and outside.

1. **Account or service hijacking:**

Credentialstheft remain top threat and attackers usually compromise the confidential, Integrity and availability of deployed critical cloud computing services.

## 2.3 Cloud Security Framework

This is an executive order established with the intention of reducing risk that are critical to infrastructure. The NIST (National Institute of Standards of Technology) policy framework is mostly used and it consists of five critical pillars: (Silk, 2021)

* **Identify:** Comprehend the organization needs and carryout security risk assessments.
* **Protect:** Implement safety measure to ensure that in the event of an attack, the infrastructure can sustain itself.
* **Detect:** setup solutions to constantly monitor the organization’s network and identify any event related to security.
* **Respond:** Capacity to instantly initiate countermeasures for cconfronting potential or active security threats.
* **Recover:** In the event of disruption of network services, create procedures needed for system restoration capabilities.

## 2.4 NIST Guidelines on Cloud Security and Privacy Issues and Recommendations

The table below was published by National Institute of Standards and Technology (NIST). It summarizes security and privacy issues in cloud computer and related recommendations which organization can follow when at different stages of public cloud outsourcing agreement. This includes planning, reviewing, negotiating stages. (Wayne Jansen, 2011)

Text

Description automatically generated with medium confidenceText

Description automatically generated

# 3.0 SECURITY RISK IN CLOUD AUTHENTICATION

The most common used authentication process in cloud environment are as follows:

* Password
* Certificates
* Tokens
* Access Keys
* One-Time Password

Different protocols are used by these authentication process. Although the implementation of these protocols is in different ways, the end goal of securing the environment remain the same while accessing the resources through unsecure Network. Some of the protocols commonly used are SAML, OAUTH, OpenID, SRP, OTP, SSH. These protocols provide at least one of the following: confidentiality, Integrity, and Availability but most of them provides all. Based on the use case, some are more effective than others.

## 3.1 Multi-factor Authentication

Simple reliance on one-factor authentication using password-based mechanism with the perils on the internet is undesirable and outdated. The threat on businesses and users now has direct link to the security of cloud-based solutions. The emergence of mobile computing has made it extremely important to develop more secure mechanism to mitigate the security risk associated with the traditional means of authentication, hence the development of multi-factor authentication which mostly take the form of 2-Factor Authentication (2FA). The 2FA is based on One-Time Password mechanism for the second authentication which comes in the form of Short Messaging Service (SMS), Quick Response codes (QR) codes, Trusted Platform Modules (TPM) and so on.

## 3.2 SAML Authentication

Security Assertion Markup Language (SMAL) is an open standard that bridges the gap between authorization and authentication. There are three main characters involves in the process, the Principal, Service provider and the Identity provider.

***The process involves***

1. The principal (that is the user) tries to access the service provider’s resources via web
2. Service provider generates authentication request to the IDP
3. The Identity Provider request SSO login to the user
4. Upon validating the user’s authentication, the IDP generate Authentication assertion and the user’s credentials to the Service provider.
5. The service provider then either allow or disallow user’s attempt to access the service depending on the IDP’s message.

Diagram

Description automatically generated

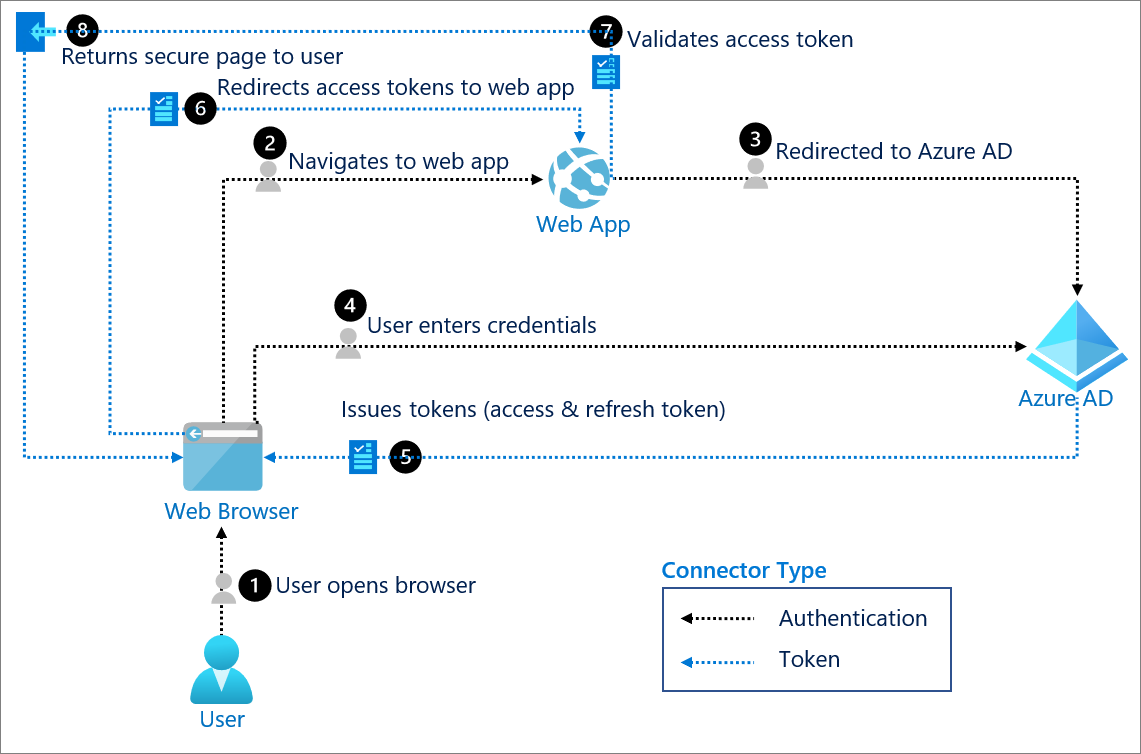
*Fig1: Diagram representation of SAML authentication flow*

SAML is used largely in Enterprises. It enables single sign-on for the users so that once signed in, the users can access other applications. “SAML simplifies the implementation of [federated authentication and authorization](https://www.hackedu.com/blog/analysis-of-common-federated-identity-protocols-openid-connect-vs-oauth-2.0-vs-saml-2.0), which involves multiple service providers across multiple organizations and security domains using a single identity provider. An example of federated identification is single sign-on (SSO). In SAML, SSO takes the form of a browser session cookie that allows access to multiple applications.” (Hunter, 2021)

## 3.3 OAuth

This protocol is an open standard for authorization that securely delegate access to API, devices, Applications and Service using Access tokens. It is important to note that OAuth give access to data, but users credentials are never accessed.

The workflow is usually between three main characters, the users, consumer, and Service provider. The flow is described in the diagram below Azure being the service provider.



*Fig2: Diagram representation of OAuth authentication flow* (Nick Ludwig, 2021)

## 3.4 OpenID

This is a protocol that is built on top of the OAuth 2.0 to provide the Authentication mechanism lacking in the OAuth. This weakness of missing Authentication in OAuth becomes more of a concern when sensitive functions are to be authorized. The workflow is listed below:

1. The third-party application(client) directs the user to the Identity Provider for authentication and authorizing access to the client.
2. The authorization code received by the client from the IDP is then used to request further for ID tokens and access.
3. When the token is obtained, the client can then perform operations on behalf of the user.

## 3.5 Security Risk involves in Using Access tokens for Authorization and authentication

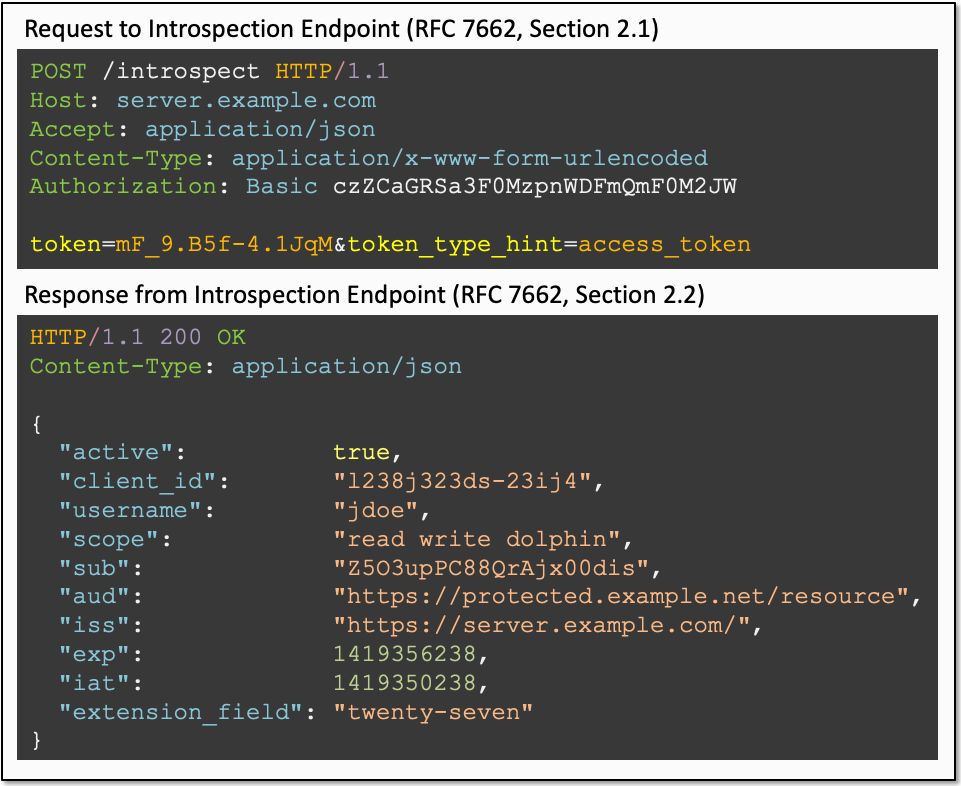
Before the advent of OAuth, the most common means of accessing systems was by using HTTP basic authentication which requires only username and password. Thereafter, Single sign-on started gaining ground when SAML became common. There was a major challenge with SAML though, it is only suitable for applications that are developed multi-paged and not suitable for applications that makes HTTP calls to APIs via webservices and AJAX. This makes using SAML for mobile applications and Internet of Things not to be ideal. However, OAuth, is perfect for modern web applications because it uses JSON packets and API calls (Hunter, 2021). For cloud Web applications that requires SSO while using OAuth protocol, an additional configuration of setting up Redirect URI for single-page apps is required (Nick Ludwig, 2021).

**OAuth Access Token**

Access Token is a piece of code that client application uses to make request to a server to get resource. Access token comes in different formats, and it may be either bearer tokens or sender-constrained token.

There are security model’s fundamental properties of OAuth access tokens:

1. Since the client app is not the audience of the token, the client must not be able to read or interpret the access tokens.
2. Users’ identity or information is not included in the access token.
3. Access tokens should be used only for making request from the resource server.



*Fig 3: Request to and Response from Introspection Endpoint (Kawasaki, 2019)*

Despite the fundamental security model for the OAuth access tokens, adversaries can still steal access token of user with the aim of acquiring the credentials to access resources and remote systems. There are different ways by which this can occur, but it typically requires user ignorantly granting access to attacker that is using social engineering technique.

The common way to access resources in software-as-a-service and cloud-based applications is through application access tokens applications which uses authorized API request on behalf of the user. OAuth framework is one of the popular implementations that issues tokens to users to access systems. Third party application is enabled by the OAuth access token to interact with resources without user credentials.

An attacker can act on the authorization given by OAuth to develop a malicious application with the objective of the application being granted access to resources with the OAuth token of the target user. The attacker’s application undergoes the required registration process with authorization server, for instance, Azure portal or REST API calls or Microsoft Identity Platform (Microsoft, Documentation, 2021). The attacker might use spear phishing link to entice the target to allow then gain access to the application. Once they succeeded in acquiring the OAuth access token, they can go further to gain long-term access into the user account if a "refresh" token which enable background access is awarded.

When access token is compromised initially, same token may be used to compromise other service. For instance, if access is granted to a victim’s email by a token, the attacker can trigger forgotten password routine on all other services that the target has subscribed for in order to extend access.my extend access to all other services. The effectiveness of second authentication is negated for direct API access through token. Also, it is immune to countermeasures like password change. This make access abuse difficult to detect even from the service provider’s end, as the access is legitimate with the workflow

# 4.0 CASE STUDY

## 4.1 Pawn Storm attacks against the Democratic National Convention (DNC)

This study is on how an aggressive group know Pawn Storm uses **Advance Social Engineering schemes** to abuse Open Authentication (OAuth). It was reported that the campaigns between 2015 and 2016 targeted high-profile user of free webmail.

The group set up credential phishing attacks against the Democratic National Convention (DNC) and the success of this attack is believed to have had a significant effect on the outcome of the United State Presidential Election of 2016 as Hilary Clinton campaign was reportedly compromised (crowdstrike, 2020).

### 4.1.1 Procedure of used to abuse OAuth

As earlier stated, OAuth is protocol use for authorizing a third-party application to sign into online accounts of the user. The online accounts can be SaaS applications, webmail services or social media sites. The main advantage of using OAuth is that user’s credentials are never revealed while the client application gets a token that is used for authentication. Although this process seems convenient looking from user’s perspective, it however exposes the user to risks. The attacker can successfully pass the background checks that the service provider does before the malicious application is authorized for OAuth use and then integrate it into advance social engineering schemes. This is how experienced criminal groups like Pawn Storm, make use of OAuth for credential phishing schemes.

Diagram

Description automatically generated

*Fig 4: The process Pawn Storm used for OAuth abuse*

User will get a message as shown below

Graphical user interface, application, Teams

Description automatically generated

*Fig 5: Sample of Email from Pawn Storm*

The email is disguised as though it is from Gmail and victims are prompted to install an “official” application called “Google Defender”.

When clicked, user is directed to a page on accounts.google.com as shown below:

Graphical user interface, application

Description automatically generated

*Fig 6: “Google Defender” access request*

The above is an authentic Google site, however, the OAuth approvals are not done on Google but rather on the service provider’s site.

It must be noted that “Google Defender” is an application by Pawn Storm and if the User fall for the scam by clicking “Allow” button, the app gain access to an OAuth token and that gives Pawn Storm access to the victim’s mailbox.

Aside from Gmail users, high-profile Yahoo users were also targeted by Pawn Storm where “McAfee Email Protection” was offered.

Graphical user interface, text, application

Description automatically generated

*Fig 7: Sample Email from Pawn Storm*

Graphical user interface, application

Description automatically generated

*Fig 8: This was never a legitimate McAfee app and same procedure as the case of “Google defender” apply in this case also when the “Agree” button is clicked.*

The chart below shows the success of Pawn Storm under the duration captured

Chart, scatter chart

Description automatically generated

*Fig 9: The blue boxes symbolizes when the attacker used OAuth lures while red boxes signify other phishing email strategies*

## 4.2 SolarWinds backdoor used in Nation-State Cyber Attacks

FireEye reported that the nation-state attack on their network was because of massive attack on SolarWinds supply chain. The threat actors reportedly gained access to numerous government and enterprise network across the globe through the backdoor campaign called “UNC2452”

"They gained access to victims via Trojanized updates to SolarWind's Orion IT monitoring and management software. This campaign may have begun as early as spring 2020 and is currently ongoing. Post-compromise activity following this supply chain compromise has included lateral movement and data theft." (FIREEYE, 2020).

Below summarizes the techniques that are part of the actor’s toolkit. (Center, 2020)

* The attacker gain access to network through malicious code in SolarWinds Orion library with the file name *SolarWinds.Orion.Core.BusinessLayer.dll.* This code gets distributed when update is sent to SolarWinds’s customers without them having any knowledge of malicious activities. The malicious DLL uses the domain avsvmcloud.com to call out a remote network. The attacker uses it to gain elevated administrator’s permission.
* The attacker then makes use of the permission obtained from the on-premises to gain access to the global administrator’s account and SAML token signing certificate. As a result of this gained access, existing users of the organization can then be impersonated by forging SAML tokens.
* Since the SAML tokens are signed by the organization’s trusted certificate, anomalous logins can be made against any cloud environment as well as on-premises resources.

Graphical user interface, text, application

Description automatically generated

*Fig 10: SolarWinds compromised Digital Signature*

* With the privileges obtained, it is easy for the attacker to add their own credentials to existing apps or service principals to enable make API calls.

### 4.2.1 Long Term Access

1. Federation Trusts: New federation trysts were added to an existing tenant to accept tokens from the attacker’s owned certificates.
2. OAuth Application and service principal credentials: x509 keys or password credentials were added to some legitimate OAuth apps within the Mail.Read or Mail.ReadWrite permission to grant ability to read mails.

# 5.0 COUNTERMEASURES AGAINST THE RISKS

## 5.1 Restriction of Web-based Content

A user must grant an application permission before it can access organization’s data. For instance, users can permit an application to access their mailbox by default, but some consent requires administrative privilege by default, like an app having read and write consent to all organization’s files (Philippe Signoret, 2022).

Administrators can disable end user’s consent to authorizing third-party application through OAuth 2.0 and made it mandatory that all requests must be approved by administrator. To reduce risk, users can be denied from registering application and by using Cloud Access Security Broker, specific applications can be ban (Jeff Sakowicz, 2019).

### 5.1.1 Configuring User consent setting on Azure

1. Login to Azure portal as Global Administrator
2. Goto Azure Active Directory – Enterprise application – Consent and Permission – User consent settings.
3. Choose the “Do not allow user consent”. By default, “Allow user consent for apps” is selected. This is risky as user can consent any app to access organization data.

Graphical user interface, text, application, email

Description automatically generated

Consent workflow can then be enabled to allow global administrator, app admin or Cloud admin to grant access (Erin Greenlee, 2022).

### 5.1.2 Prevent Users from Registering new applications

1. Login to Azure portal as Global Administrator
2. Go to Users- User settings
3. Under “App registrations”, Select “No”

Graphical user interface, text, application

Description automatically generated

## 5.2 User Training

Humans are fallible and makes mistake. It is therefore necessary to train users on the need not to authorize third party application they do not know. It is important to train users on how attacker conduct their malicious activities, like the need to pay attention to redirect URL, Misspelt URL, spotting a website trying to spoof a legitimate. Users are to be made to understand the risk involved in granting access to applications that request for consent to read emails because SaaS APIs can be used by attackers to acquire user’s credentials and other sensitive data.

The Method use in training is also of great importance to ensure positive outcome. Older people learn better when something applies to their real lives, the educational guide need to target this aspect. Also, training should be practical based to ensure retentiveness.

## 5.3 Setup Automated Response

Microsoft Azure Active Directive has features that automatically intercept attacks. The time space between detection and response is significantly reduced by using these features.

### Sign-in risk policy

This solution measures the chances that an authentication request is not legitimately authorized by a user. Conditional access policy is configured which evaluate the level of risk to either group or user. Different access policies can be configured, it includes, user’s location, if/when MFA is required on medium or high risky logins etc.

Graphical user interface, text, application, email

Description automatically generated`

*Fig 11: Implementing Conditional Access on Azure portal*

**5.4 Table below capture the two case studies and provides general overview.**

***5.4.1 Democratic National Convention (DNC)***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Threat actor | Threat | Vulnerability | Technical Impacts | Business Impact | Controls |  |  |
| External  Potential threat  actors that might gain unauthorized  access to customer PII. | Account Hijacking and data leakage | Lack of Administrative control regarding permission on app access consent. | Sensitive Data Breach: Loss of credentials, exposure of sensitive PII data | Reputational  -The incident was believed to have cost Hilary Clinton the presidential Election for lack of integrity. | Prevention  -User Awareness  - Control measure on token access by users |  |  |
|  |  | Effective monitoring and auditing to check and maintain only necessary permission was not in-place |  | Operational  -Forensics Analysis  - Campaign process stalled due to incident response | Detective  -Auditing  - Using Monitoring tools that triggers severity alerts when apps require too sensitive access from users. |  |  |
|  |  |  |  | Financial  -Due to added operational cost.  -Less donation after the breach |  |  |  |

***5.4.2 SOLARWINDS***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Threat actor | Threat | Vulnerability | Technical Impacts | Business Impact | Controls |
| Internal  Design and human error by software development team. | *Cloud Services*  *and Credentials*  *Compromise:*  Attacker  was able to  compromise multiple customer’s Azure and other cloud and on-premises Network | Misconfiguration that left a backdoor for adversary to explore | Exposure of  sensitive personal,  company, and  government data. | Financial  The attack cost SolarWinds about 11% of the annual revenue | Prevention  -Removing and disabling unnecessary applications and service principals.  -Following best practice of identity federation provider to secure SAML tokens. |
| External  Malicious Hacker: Nation-State Cyber Attacker | Lack of adequate oversight. | Effective monitoring and auditing to carryout security checks and maintain necessary permission was not in-place | Loss of credentials | Compliance  GDPR breached | Detective  -Running up to date Antivirus that detect compromised SolarWinds Library.  - Monitor anomaly usage of service account. |
|  |  |  |  | Operational  -Running extensive investigation of the network to check for compromised data |  |

# 6.0 CONCLUSION

The advantages that come with cloud computing technology is enormous reason for its rapid popularity among consumers. Unfortunately, these merits do come along with some problems too and security is one of the major challenges. The main selling points of cloud computing is the ease of accessibility, this make different authentication techniques framework that make user experience easy and seamless as possible to be implemented and this exposes users to more risk, making them vulnerable to attacks.

Reasons for most breaches has been due to accidental exposing data or compromised channel. Due to more usage of applications and platform enabling web technology on cloud, Application APIs are now more sophisticated which malicious users use to exploit victims by stealing access and/or manipulating user access tokens for their benefits. In the report, some methodologies attackers use to carried out attacks on victims was analyzed and recommended countermeasures where provided which includes limiting end user permission in granting applications access for OAuth authentication, reducing surface area by disabling unnecessary apps, User training and effective monitoring/ Auditing. This will go a long way to protecting data, maintaining Integrity, and ensuring that our resources are available when needed.

# 8.0 References

Center, M. S. (2020, December 13). *Blog*. Retrieved March 6, 2022 from Microsoft Inc: https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

crowdstrike. (2020, June 5). *Blog*. Retrieved March 5, 2022 from https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Erin Greenlee, P. S. (2022, February 8). *Documentation*. Retrieved March 7, 2022 from Microsoft inc: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow

FIREEYE. (2020, December 13). *Resources*. Retrieved March 7, 2022 from mandiant: https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

Hunter, A. (2021, April 2). *RAS*. Retrieved March 3, 2022 from Parallels International GmbH.: https://www.parallels.com

Irena Bojanova, J. Z. (2013). Cloud Computing. 13. Retrieved February 20, 2022

Jeff Sakowicz, M. W. (2019, September 4). *Mitigations*. Retrieved March 7, 2022 from The MITRE Corporation: https://attack.mitre.org/techniques/T1528/

Kawasaki, T. (2019, May 21). *Darutk*. Retrieved March 6, 2022 from Medium: https://darutk.medium.com/oauth-access-token-implementation-30c2e8b90ff0

Liliana F. B. Soares, D. A. (2013). *Secure User Authentication in Cloud Computing Management Interfaces.* Covilhã, Portugal: Rua Marquês d’Ávila e Bolama, 6201-001. Retrieved 02 21, 2022

Michael Kretzschmar, M. G. (2011). Security Management Areas in the Inter-Cloud. *4th International Conference on Cloud Computing* (pp. 1-2). Germany: IEEE Computer Society. Retrieved February 20, 2022

Microsoft. (2021, 1 14). *Documentation*. Retrieved 3 1, 2022 from Microsoft Inc: https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

Ms.Neha Mahakalkar, M. S. (2017). *Implementation of Re-encryption Based Security Mechanism to Authenticate Shared Access in Cloud Computing.* India: International Conference on Trends in Electronics and Informatics. Retrieved February 21, 2022

Nick Ludwig, M. M. (2021, 3 14). *OAuth 2.0: Documentation*. Retrieved 3 1, 2022 from Microsoft Inc: https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-flow#redirect-uri-setup-required-for-single-page-apps

P.Mell and T. Grance. (2009.). “The nist definition of cloud computing,” , vol. 53, no. 6, article 50,. *National Institute of Standards and Technology*, 6. Retrieved 02 19, 2022

Philippe Signoret, J. O. (2022, January 20). *Documentation*. Retrieved March 7, 2022 from Microsoft Inc: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent?tabs=azure-portal

Rajani Sharma, R. K. (2014). *Cloud Computing –Security Issues, Solution and.* India: International Journal of Engineering Research.

Riddhi Doshi, V. K. (2020). Security Concerns in Cloud Computing and Proposed Security Models. *Security Concerns in Cloud Computing and Proposed Security Models*, 2-4. Retrieved February 20, 2022

Silk, G. (2021, November 5). *Blog*. Retrieved March 1, 2022 from Uptycs: https://www.uptycs.com/blog/what-is-a-cloud-security-framework

SUN, P. J. (2019). *Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions.* China: Digital Object Identifier 10.1109/ACCESS.2019.2946185. Retrieved 02 21, 2022

Wayne Jansen, T. G. (2011). *Guidelines on Security and Privacy in Public Cloud Computing.* Washington: NIST Special Publication 800-144. Retrieved March 7, 2022

Williams Starllings, L. B. (2015). *Computer Security Principle and Practice* (Third ed.). New Jersey: Pearson Education, Inc. Retrieved March 4, 2022