International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 56 No. 2 April 2026, pp. 209-215

Introduction Aux Concepts De La Sécurité : Authentification Et Autorisation

[1]Mbengi Ngoma joachim, [2]Mavungu N'luangu jean camile, [3]Muhima wa Tebo, [4]Mansiantima Lutete doris, [5]Mbuyamba Tshunza roger

[1]Chef de travaux au Département de Physique et Sciences Appliquées, Doctorant en Génie Informatique, Faculté des Sciences et Technologies Université Pédagogique Nationale, BP 8815, Kinshasa, RD Congo

[2]Assistant au Département de Physique et Sciences Appliquées, Faculté des Sciences et Technologies Université Pédagogique Nationale, BP 8815, Kinshasa, RD Congo

[3]Professeur Associé à la Faculté des Sciences et Technologies Université Pédagogique Nationale, BP 8815, Kinshasa, RD Congo

[4]Professeur au Département de Physique et Sciences Appliquées, Faculté des Sciences et Technologies Université Pédagogique Nationale, BP 8815, Kinshasa, RD Congo

[5]Professeur au Département de Physique et Sciences Appliquées, Faculté des Sciences et Technologies Université Pédagogique Nationale, BP 8815, Kinshasa, RD Congo

Corresponding Author: Mbengi Ngoma Joachim

Résumé : La sécurité est très capitale dans la vie humaine du fait qu'elle permet à ce que l'homme se protège et ce qu'il procède contre les détracteurs, malveillants et autres ...

En informatique, les données et le système sont des mannes qu'il faut protéger à tout prix, c'est la raison d'être de la sécurité informatique.

Dans le domaine de la sécurité informatique, deux concepts fondamentaux très important qu'il faut tenir compte pour la protection des données et système : l'authentification et l'autorisation.

Ces concepts fondamentaux bien que distincts mais sont interdépendant et permettent de renforcer la sécurité du système dans son ensemble et faire que les ressources soient consultées par des personnes sûres et au bon moment.

Mots clés : authentification, autorisation

L'article introduit deux concepts fondamentaux de la sécurité informatique : l'authentification et l'autorisation.

- ***L'authentification*** **consiste à vérifier l'identité d'un utilisateur, généralement à l'aide d'un mot de passe, d'un badge, d'une empreinte biométrique ou d'un système à double facteur.**
- **L'autorisation, quant à elle, détermine les droits d'accès d'un utilisateur authentifié aux ressources (fichiers, applications, services).**

Ces deux processus sont complémentaires : l'un identifie, l'autre donne ou restreint l'accès. Leur bonne mise en œuvre est essentielle pour protéger les systèmes contre les accès non autorisés et garantir la confidentialité, l'intégrité et la disponibilité des données.

Abstrat: Security is very important in humain life because it allows man to protect himself and what he does against detractors, malicious and others ...

ln computing, data and the system are manna that must be protected at all costs, this is the reason for computer security .

In the field of computer security, two fundamental concepts are very important that must be taken into account for the protection of data and system: authentication and authorization.

These fondamental concepts, altnough distinct, are complementary and make it possible to strengthen the security of the system as a whole and ensure that resources are consulted by safe people and at the right time.

Keywords : authentication, autho1"ilntion

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 56 No. 2 April 2026, pp. 209-215

Introduction

Dans le domaine de la cybersécurité, deux concepts essentiels se distinguent lorsqu'il s'agit de protéger les systèmes et les données : l'authentification et l'autorisation. Ces deux notions relèvent de la gestion des identités et des accès, également connue sous le nom d'Identity and Access Management (IAM). Bien qu'on les utilise souvent ensemble et qu'elles soient parfois confondues mais elles ont des objectifs distincts.

L'authentification et l'autorisation représentent des processus spécifiques qui jouent chacun un rôle fondamental pour contrôler l'accès aux informations. Comprendre la fonction de chacun est crucial pour garantir la sécurité des données et pour permettre à une organisation de prendre des décisions éclairées en matière de cybersécurité.

Cet article vise à clarifier ces deux concepts en détaillant leur signification, leurs différences et leurs importances pour la protection des systèmes Informatiques.

1. Authentification et autorisation

1.1. Authentification

L'authentification est le processus de vérification de la validité d'une identité déclarée. Elle implique que l'utilisateur fournisse des informations additionnelles qui doivent correspondre précisément à l'identité revendiquée. Ce mécanisme permet aux utilisateurs de démontrer qu'ils sont bien ceux qu'ils prétendent être.

Lors d'une tentative de connexion, l'authentification consiste à valider les informations d'identification de l'utilisateur. Cette procédure inclut l'envoi des informations d'identification du client (telles qu'un nom d'utilisateur et un mot de passe) vers le serveur d'accès réseau, soit en texte clair, soit sous forme chiffrée par un protocole d'authentification. Et l'identité est vérifiée en la comparant avec un compte de domaine pour confirmation.

1.2. Autorisation

L'autorisation intervient une fois que l'authentification a été effectuée. Après avoir vérifié une identité, il faut déterminer ce que cette identité est autorisée à faire dans un système spécifique. L'autorisation assure que les actions demandées ou l'accès à une ressource sont permis en fonction des droits et des privilèges accordés à l'identité authentifiée.

Le système examine généralement une matrice de contrôle d'accès. qui évalue la relation entre le sujet, l'objet et l'action envisagée. Si l'opération demandée est permise, le sujet obtient l'autorisation nécessaire. Si l'opération est interdite, l'accès est refusé.

2. Matériels et méthodes

2.1. Les Méthodes courantes d'authentification

L'authentification repose souvent sur l'utilisation de différents facteurs, qui se divisent en trois grandes catégories :

ce qu'est l'utilisateur : il s'agit d'informations comme des mots de passe, des codes PIN ou des réponses à des questions de sécurité ;

ce que l'utilisateur possède : Cela inclut des objets physiques tels qu'une carte d'identité, un smartphone équipé d'une application d'authentification, ou un token matériel

ce que l'utilisateur est : Ce sont des caractéristiques biométriques, telles que les empreintes digitales, la reconnaissance faciale, la voix ou la lecture de la rétine.

Pour renforcer la sécurité et diminuer le risque d'accès non autorisé, on privilégie de plus en plus l'authentification multi-facteurs (MFA), qui combine plusieurs de ces éléments.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 56 No. 2 April 2026, pp. 209-215

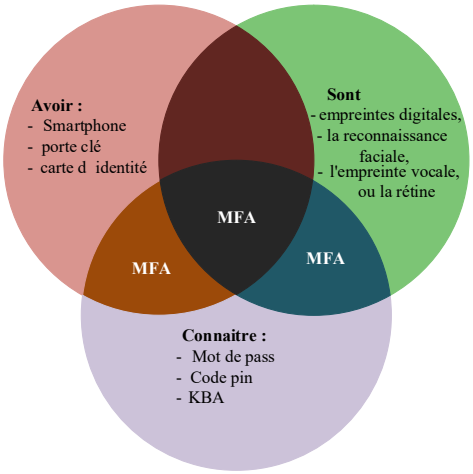

Figure 1 : la représentation de différents méthode d'authentification avec la jonction de deux ou trois méthodes qui représente l'authentification multifacteur

a. Mots de passe

Les mots de passe restent le moyen d'authentification le plus couramment utilisé aujourd'hui. Ils se divisent en deux types : les mots de passe statiques et les mots de passe dynamiques.

Les mots de passe statiques sont des identifiants qui ne changent pas et sont utilisés pour de multiples connexions sur le même compte. Bien que cette méthode soit la plus courante dans les entreprises, elle est également ln moins sécurisée. Pour cette raison, les entreprises devraient limiter l'usage des mots de passe statiques à l'authentification locale, car les techniques pour intercepter un mot de passe qui circule sur un réseau sont nombreuses et relativement faciles à exploiter.

Pour pallier aux faiblesses des mots de passe statiques, l'authentification à deux facteurs a émergé. Elle combine deux éléments - « ce que je possède » et « ce que je sais » - pour renforcer la sécurité.

Dans ce cas, les mots de passe sont générés par des dispositifs qui nécessitent un code PIN (Personal Identification Number) pour s'activer. Avec un mot de passe dynamique, chaque mot de passe généré est valable une seul fois, ce qui rend sa capture inefficace : une fois utilisé, le mot de passe expire immédiatement.

Les mots de passe à usage unique (ou One Time Password, OTP) sont un exemple de mots de passe dynamiques. Le programme SKEY, par exemple, utilise une fonction à sens unique pour générer un mot de passe différent à chaque connexion.

Pour améliorer la sécurité des accès utilisateurs aux systèmes d'information, il est recommandé de combiner l'authentification forte (comme les mots de passe à usage unique, les certificats X.509, ou des solutions biométriques) avec un serveur SSO (Single Sign-On), en fonction du niveau de sensibilité des données à protéger.

De plus, il est possible de sécuriser les mots de passe statiques lors de leur transmission sur un réseau en utilisant des protocoles d'authentification réseau comme Kerberos, qui garantit une meilleure protection des données d'identification.

b. Certificats de clés publiques

La cryptographie à clé publique permet de chiffrer des mots de passe, mais elle sert également à signer des données. Cela peut inclure, par exemple, un contrat, pour que les signataires ne puissent pas renier leur engagement par la suite, ou encore un jeton aléatoire pour des besoins d'authentification.

Les certificats de clés publiques sont aujourd'hui une méthode d'authentification répandue, bien qu'ils restent moins courants que les mots de passe. Toutefois, leur popularité ne cesse de croître. La cryptographie asymétrique repose sur deux clés liées mathématiquement : une clé publique et une clé privée.

(1) La clé publique

- est accessible à tous ;
- est utilisée par ceux qui souhaitent vérifier la signature d'un document électronique signé avec la clé privée correspondante assurant ainsi l'authenticité et l'intégrité du fichier ;
- permet de chiffrer un message pour qu'il ne soit lisible que par le détenteur de la clé privée associée.

(2) La clé privée :

- doit rester secrète et être conservée par son propriétaire ;
- sert à signer électroniquement des documents (messages, contrats. etc.) ;
- est utilisée pour déchiffrer des messages qui lui sont destinés, chiffrés avec la clé publique.

Avec la clé publique, il est pratiquement impossible de déduire la clé privée correspondante dans un délai raisonnable avec des moyens courants (par exemple, en une journée avec un seul ordinateur). Cette sécurité repose sur la relation de confiance entre l'utilisateur et sa paire de clés (clé publique et clé privée), appelée certificat. Ce certificat est un fichier contenant des paramètres cryptographiques (comme l'algorithme utilisé et la taille des clés) et des informations d'identification, validées par une autorité tierce connue sous le nom d'Autorité de Certification (AC), qui signe le certificat.

Pour vérifier l'identité d'une personne et la validité de sa signature électronique, il est nécessaire d'examiner le certificat X.509 associé à la clé de signature et de remonter la chaîne de certification jusqu'au certificat racine de l'Autorité de Certification (un certificat auto-signé). La question qui reste est donc de savoir où trouver ces certificats pour effectuer la vérification.

c. Biométrie

La biométrie est l'une des méthodes les plus fiables et couramment utilisées pour la reconnaissance et l'authentification des individus. Cette discipline repose sur l'analyse des caractéristiques biologiques, physiques ou comportementales des personnes, comme l'ADN, la voix, les empreintes digitales, la forme du visage, la forme des mains, la démarche, etc. Les techniques biométriques basées sur des caractéristiques biologiques (comme l'ADN, la salive, l'urine, ou les odeurs) sont coûteuses et complexes à déployer pour un usage quotidien. Il existe aussi deux autres types de méthodes biométriques : physiologiques et comportementales.

Grâce à sa robustesse, sa fiabilité et sa capacité à s'intégrer facilement dans de nombreux systèmes de sécurité et de contrôle d'accès, la biométrie occupe aujourd'hui une place de choix parmi les technologies de sécurité avancée en constante évolution.

2.2. Les Méthodes d'autorisation courantes

L'autorisation est le processus qui permet d'accorder à une personne l'accès à une ressource numérique. Dans les entreprises, existe plusieurs méthodes pour gérer l'autorisation d'accès des utilisateurs :

- contrôles d'accès basés sur les rôles (RBAC) : Cette approche traditionnelle attribue les permissions d'accès en fonction des rôles des utilisateurs. Par exemple, les membres du département des ressources humaines peuvent avoir accès à une application de gestion de la paie, tandis que ceux du service financier peuvent accéder aux outils de création de rapports financiers. Le RBAC est adapté lorsque l'accès est limité aux utilisateurs internes et au sein d'un réseau restreint, mais il devient trop rigide dans de nombreuses situations modernes ;
- contrôles d'accès basés sur les attributs (ABAC) : L'ABAC surmonte certaines des limitations du RBAC en prenant en compte des attributs supplémentaires pour déterminer les droits d'accès. Cette méthode offre une plus grande flexibilité et sécurité, en évaluant des informations variées telles que les attributs de l'utilisateur comme âge, niveau de sécurité, les caractéristiques des ressources (cas de date de création, type de ressource) et le contexte d'accès : lieu et heure d'accès.

2.3. Différences entre Authentification et Autorisation

- L'authentification permet de confirmer l'identité d'un utilisateur, tandis que l'autorisation détermine les actions ou ressources auxquelles cet utilisateur a droit ;

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/ Vol. 56 No. 2 April 2026, pp. 209-215

- L'authentification précède généralement l'autorisation : sans une authentification réussie, l'accès aux ressources n'est généralement pas accordé ;
- L'authentification repose sur des preuves d'identité, tandis que l'autorisation s'appuie sur des règles et des politiques d'accès ;
- L'authentification est souvent centralisée (par exemple, via un annuaire LDAP), alors que l'autorisation peut être décentralisée et adaptée aux ressources spécifiques.

Dans le domaine de la gestion de l'identité et de la sécurité des données, l'authentification et l'autorisation sont deux processus complémentaires qui garantissent qu'un utilisateur puisse accéder à une application ou un système de manière appropriée. Ces deux mécanismes visent à protéger les systèmes en s'assurant que seuls les utilisateurs autorisés accèdent aux informations ou ressources appropriées.

Dans le cadre de la gestion des identités et des accès (1AM), l'authentification concerne la vérification de l'identité d'un utilisateur, tandis que l'autorisation se concentre sur la gestion des droits d'accès. L'authentification est la première étape de l'interaction en ligne, exigeant des utilisateurs qu'ils fournissent leurs identifiants pour prouver leur identité. Ensuite, l'autorisation intervient pour appliquer les politiques qui déterminent quelles ressources l'utilisateur est autorisé à consulter ou à modifier.

3. Les Protocoles de d'authentification et d'autorisation utilisés

3.1. Protocole RADIUS (Remote Authentification Dial-In User Service)

Le protocole RADIUS repose sur une architecture client/serveur et offre des services d'authentification, d'autorisation et de gestion des comptes lors d'accès à distance. Le cas d'un utilisateur nomade qui souhaite se connecter à un réseau interne via un canal sécurisé, tel qu'un VPN (Virtual Private Network). Le processus d'authentification avec RADIUS se déroule comme suit :

(1) l'utilisateur initie une requête de connexion. Le routeur d'accès à distance (client RADIUS) collecte les informations d'identification, comme le nom d'utilisateur et le mot de passe ;
(2) ces informations sont envoyées au serveur RADIUS ;
(3) le serveur RADIUS reçoit la demande, la vérifie et renvoie la configuration nécessaire pour autoriser ou non l'accès au réseau ;
(4) en fonction de la réponse du serveur RADIUS, l'utilisateur reçoit soit un message d'erreur en cas d'échec, soit un message indiquant l'accès accordé s'il a été authentifié avec accès.

3.2. Protocole SSL (Secure Socket Layer)

Le SSL, développé par Netscape et RSA Data Security Inc., est conçu pour sécuriser les communications sur des protocoles TCP/IP, comme HTTP, FTP, LDAP, SNMP, Telnet, etc. En pratique, il est principalement utilisé avec LDAPS et HTTPS. SSL fournit des services d'authentification, de confidentialité et d'intégrité. Voici comment s'opère l'authentification avec SSL :

(1) le client (navigateur) demande une transaction sécurisée avec le serveur ;
(2) en réponse, le serveur envoie son certificat au client ;
(3) le serveur propose une liste d'algorithmes cryptographiques possibles pour la négociation;
(4) le client sélectionne un algorithme ;
(5) le serveur envoie à son tour son certificat, accompagné des clés cryptographiques correspondantes ;
(6) le navigateur vérifie la validité du certificat ;
(7) si validé, le client envoie une clé secrète chiffrée avec la clé publique du serveur, qui pourra la déchiffré et utiliser cette clé pour échanger des données en toute sécurité.

Afin d'éviter les attaques, il est recommandé de mettre en place une double authentification, combinant l'authentification du serveur et celle du client, bien que l'authentification du client ne soit pas obligatoire avec SSL.

Le protocole TLS (Transport Layer Security) est la version normalisée de SSL 3.0, et les versions de TLS continuent d'évoluer pour répondre aux nouvelles vulnérabilités.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 56 No. 2 April 2026, pp. 209-215

3.3. Kerberos

Kerberos est un protocole conçu pour assurer à la fois l'authentification et l'autorisation, permettant ainsi de valider non seulement l'identité d'un utilisateur, mais aussi ses droits d'accès. Très utilisé pour le Single Sign-On (SSO), Kerberos ne transmet jamais de mots de passe sur le réseau, mais utilise un chiffrement symétrique avec des clés secrètes et un service tiers pour authentifier les identités des utilisateurs et des applications.

Ce protocole fonctionne en arrière-plan de manière presque transparente pour l'utilisateur : une fois authentifié, l'utilisateur peut accéder aux ressources réseau et applications tierces sans devoir se reconnecter à chaque fois.

3.4. LDAP (Lightweight Directory Access Protocol)

LDAP a été conçu pour fournir une authentification sécurisée et stocker les informations des utilisateurs de manière hiérarchique dans un annuaire. Il est souvent utilisé dans les environnements Active Directory pour gérer l'accès et l'organisation des ressources. Les utilisateurs se connectent à un serveur LDAP pour vérifier leurs informations et accéder aux ressources, les permissions étant gérées directement au sein de l'annuaire, sans nécessité d'intervention de l'administrateur.

3.5. Protocole WTLS (Wireless Transport Layer Security)

WTLS est une adaptation du TLS pour les réseaux sans fil. Les négociations entre le client et le serveur ont été modifiées pour mieux s'adapter aux contraintes des réseaux mobiles. Cela inclut la réduction des en-têtes et une meilleure compression des données pour optimiser l'utilisation de la bande passante.

Le processus d'authentification dans WTLS implique la conversion des données entre le format WTLS et SSL/TLS par une passerelle WAP, assurant ainsi la sécurité des communications entre un appareil mobile et le serveur web.

3.6. WS-Trust

Le protocole WS-Trust permet d'é1ablir des relations de confiance entre applications ou terminaux en gérant des jetons de sécurité via un service tiers appelé Security Token Service (STS). Ce protocole est utilisé pour sécuriser les communications entre différentes entités en validant et renouvelant des jetons de sécurité facilitant ainsi la gestion des identités et l'accès sécurisé aux services web.

3.7. Protocole 802.lX-EAP

Le protocole 802.1 X-EAP est un 111écanisme standard pour l'authentification mutuelle entre un client et un composant réseau (comme un commutateur ou un point d'accès sans fil). li utilise un serveur d'authentification, souvent basé sur RADIUS, et l'un des protocoles EAP pour assurer une authentification solide et dériver des clés de chiffrement pour sécuriser les sessions réseau .

Conclusion

Dans un environnement numérique en constante évolution, où la protection des données est une priorité cruciale, il est essentiel de bien comprendre les principes d'authentification et d'autorisation pour concevoir des systèmes à la fois sûrs et performants. Bien que ces deux processus soient distincts, ils se complètent mutuellement pour renforcer la sécurité globale, en garantissant que seules les personnes autorisées aient accès aux ressources appropriées, et ce, au moment voulu. En adoptant des pratiques solides d'authentification et d'autorisation, les organisations peuvent se prémunir contre les risques internes et externes, tout en assurant la confidentialité, l'intégrité et la disponibilité des informations.

Référence

[1]. Pillou, J-F. et Bay, J-P. (2016). Sécurité Informatique, 4e éd. Paris Dunod, France

[2]. Pujolle G., (2008). Les réseaux, éd. EYROLLES, Paris

[3]. Rajaonarison, T. F. (2018). Accès sécurisé avec VPN a des services de systèmes distribues par cluster computing, Mémoire Master Télécom, Université d'ANTANANARIVO, Madagascar

[4]. Rasamimisa, H. H. et al, (2005). La sécurité dans les réseaux informatiques, Antananarivo, Mémoire de Master Electronique

[5]. Rigney, C., Willens, S., Ruhens, A.et al. (2000). https://tools.ietf.org/html/rfc2865 consulté le 22/04/2020 à 09 :24

[6]. Stewart E. L., (2009). CCNA Security, Pearson Education. Inc

[7]. Trouchaud P. (2016). La cybersécurité au-delà de la technologie, Odile Jacob, Paris

[8]. Tutoriel OpenVPN : Installation, configuration du serveur VPN et connexion| ITIGIC, Consulté le 08 janvier 2021

[9]. Melle TSSIAKHEM Amel & Melle M'RAH Maria, Etude & mise en place d'une solution pour la sécurisation périphérique, Mémoire de Master, 2023

[10]. https://www.keepersecurity.com/blog/fr/2023/05/15/the-pros-and-cons-of-a-vpn consulté le 19/01/2025 à 04 :22

[11]. https://www.keepersecurity.com/blog/fr/2023/04/05/three-ways-vpns-make-remote-access-less-secure/ le 19/01/2025 à 04 :27

[12]. https://www.paloaltonetworks.fr/cyberpedia/what-is-a-business-vpn-understand-its-uses-and-limitations le 19/01/2025 à 04 :34

[13]. www.openssl.org

[14]. https://www.keepersecurity.com/blog/fr/2024/03/19/the-differents-types-of-authorization-model/

[15]. https://www.pingidentity.com/fr/resources/identity-fundamentals/authorization/ authorization-methods.html

[16]. https://www.pingidentity.com/fr/resources/identity-fundamentals/authentication- authorization-protocols.htm /