ESATI

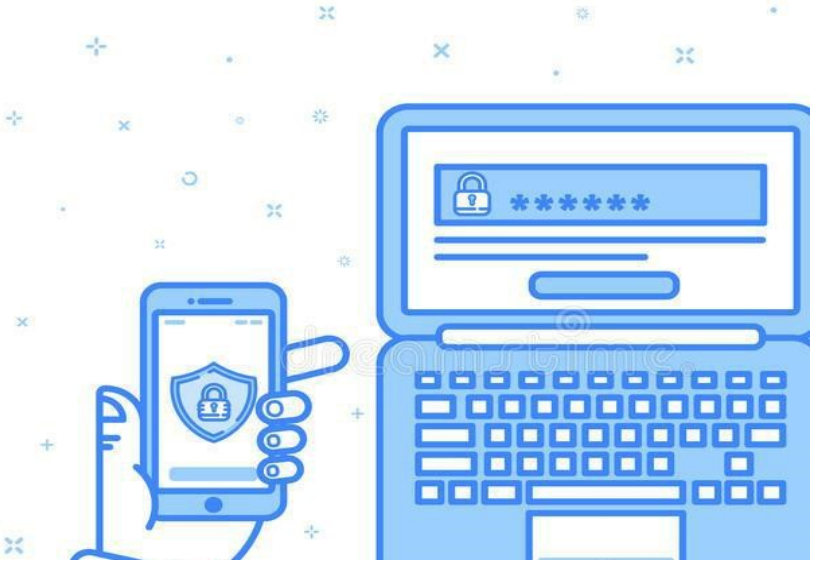
Club D

Ministère de l'Economie Numéri

TRAVAUX MASTER I

SECURITE DES SYSTEMES D'INFORMATIONS

AUTHENTIFICATION A DOUBLE FACTEURS



ETUDIANTS :

AHISSAN Oi AHISSAN SAMUEL

COULIBALY ISSOUF

KONE ABDALLAH HAKIM

PLAN DU TRAVAIL

- INTRODCUCTION

I- GENERALITES ET PRESENTATION DES SYSTEMES D'AUTHENTIFICATION

II- QUELQUES SOLUTIONS CONCERNANT LA MISE EN PLACE DES SYSTEMES A DOUBLE FACTEURS

III- EXEMPLE D'AUTHENTIFICATION A DOUBLE FACTEURS

- CONCLUSION

INTRODUCTION

La sécurité d'un système d'informations est un état dans lequel les entités possèdent un niveau d'exposition minimale au risque. Dans le domaine informatique, bon nombre de mécanismes ont été implémenté et s'appliquent à différents niveaux des systèmes notamment au niveau de l'authentification des utilisateurs. L'accès au système est sanctionné pour une identité claire et précise des utilisateurs. Mais les attaques et les techniques d'intrusion se faisant de plus en plus efficaces sur les méthodes d'authentification classiques, des systèmes d'authentification multi-facteurs ont vu le jour. Dans les lignes qui suivent, nous nous pencherons sur le cas particulier de l'authentification double facteurs.

En premier lieu nous présenterons l'authentification sur un cadre général pour déboucher l'authentification à double facteurs en montrant ses forces et faiblesses. En second lieu, nous parlerons des solutions existantes pour déployer cette technologie et nous exposerons un cas pratique d'implémentation.

I- GENERALITES

1- Présentation de l'authentification

L'authentification est un processus visant à confirmer qu'une entité est bien légitime pour accéder aux ressources d'un système (systèmes, réseaux, applications…). Et cela s'oppose à l'identification d'une personne physique ou morale (dirigeant et toute personne autorisée). Cette distinction est importante puisque par abus de langage, on parle d'authentification alors qu'il s'agit d'identification. En effet lorsqu'une personne présente sa pièce d'identité lors d'un contrôle, elle est identifiée grâce à un document officiel, mais n'est pas authentifiée, car le lien entre la pièce d'identité et la personne n'est pas établie de façon indiscutable, irrévocable et reconnue par les tribunaux en cas de litige. Lorsqu'une personne est authentifiée, cette authentification doit être apportée par un tiers de confiance et par une preuve au sens juridique reconnue devant les tribunaux (ex. : la signature électronique de la carte bancaire).

Il existe quatre facteurs d'authentification classiques qui peuvent être utilisés dans le processus d'authentification d'un commettant :

- Facteur mémoriel (ce qu'il sait)

  Empreinte : une information qu'il a mémorisé.
  Exemples : le nom de sa mère ou un mot de passe.
- Facteur matériel (ce qu'il possède)

  Empreinte : une information contenue dans un objet qu'il utilise.
  Exemples : une clé USB, un identifiant sur bande magnétique, un certificat numérique sur une carte à puce.
- Facteur corporel (ce qu'il montre)

  Empreinte : une trace corporelle qu'il peut laisser quelque part.
  Exemples : une empreinte digitale, les caractéristiques de sa pupille, sa voix.
- Facteur réactionnel (ce qu'il fait)

  Empreinte : un geste qu'il peut reproduire.
  Exemples : sa signature.

D'autres facteurs d'authentification peuvent parfois être utilisés comme les contraintes temporelles ou les capacités de localisation.

Le contrôle permanent de l'intégrité et de l'accès (usage, identité du destinataire, émetteur, propriétaire) à un contenu ou à un service constitue le fondement de la traçabilité des transactions. Ce contrôle permet :

- La protection des intérêts supérieurs de l'État et du patrimoine informatique des entreprises, donc de leurs intérêts commerciaux ; pour les entreprises, il s'agit

de réduire le coût qui résulte d'attaques, de la perte de temps, de la perte d'informations, de l'espionnage ou des fuites involontaires d'informations ;

- Le développement du commerce et des échanges électroniques. L'authentification contribue à la facturation des services et contribue à la confiance dans l'économie numérique, condition indispensable du développement économique ;

- La protection de la vie privée. Les données personnelles véhiculées dans les systèmes d'information sont des données sensibles à protéger.

2- Authentification double facteurs

La double authentification (Two-factor authentication en anglais, 2FA) ou vérification en deux étapes est une méthode par laquelle un utilisateur peut accéder à une ressource informatique (un ordinateur, un téléphone intelligent ou encore un site web) après avoir présenté deux preuves d'identité distinctes à un mécanisme d'authentification. Généralement l'une se présente sous la forme d'un jeton physique, comme une carte, et l'autre sous forme d'informations mémorisées, par exemple un code de sécurité. Ces deux facteurs représentent une chose possédée et une chose sue. Par exemple, Une carte bancaire est un bon exemple d'authentification à double facteur
: la carte elle-même constitue l'élément physique, tandis que le code secret (ou PIN) représente les données qui y sont associées. La combinaison de ces deux éléments rend plus difficile l'accès à un compte bancaire par une personne non autorisée, celle-ci devant posséder à la fois l'élément physique (la carte) et le code secret. Ce type d'authentification permet de réduire l'incidence de fraudes en ligne, telles que l'usurpation d'identité et l'hameçonnage, étant donné que le mot de passe de la victime ne suffit pas à accéder aux informations

3- Force et faiblesse

➢ Force

Le mot de passe est actuellement le système le plus couramment utilisé pour authentifier un utilisateur. Il n'offre plus le niveau de sécurité requis pour assurer la protection de biens informatiques sensibles, car différentes techniques d'attaque permettent de le trouver facilement. On recense plusieurs catégories d'attaques informatiques pour obtenir un mot de passe :

-Attaque par force brute ;

-Attaque par dictionnaire ;

-Ecoute du clavier informatique (keylogger), par voie logicielle (cheval de troie...), ou par écoute distante (champ électrique des claviers filaires, ou ondes radio faiblement chiffrées pour les claviers sans fils3) ;

-Ecoute du réseau (password sniffer) : plus facilement avec les protocoles réseau sans chiffrement, comme HTTP, Telnet, FTP, LDAP, etc ;

-Hameçonnage (ou filoutage), appelé en anglais phishing ;

-Attaque de l'homme du milieu ou man in the middle attack (MITM) : par exemple avec les protocoles SSL ou SSH ;

-Ingénierie sociale ;

-Extorsion d'informations par torture, chantage ou menaces.

Le mot de passe, à lui seul, n'étant pas une solution assez sûre, car en cas de vol de mot de passe (via une attaque man in the middle, un phishing ou autre), il n'y a plus de barrière qui s'oppose au criminel qui veut se connecter sur l'un de vos comptes. Et cela peut avoir des conséquences dramatiques comme le vol d'argent (PayPal, la banque…etc.), ou l'usurpation d'identité (Twitter, Facebook, votre boite mail…etc.)

L''authentification à deux facteurs viens ajouter une couche de sécurité supplémentaire. En plus de l'élément que "vous connaissez", il y a l'élément que "vous avez" comme par exemple un téléphone mobile ou un ordinateur. Même si ce dernier peut changer de mains, il n'est pas une condition suffisante et c'est la combinaison du "vous connaissez" et du "vous avez" qui constitue la base de l'authentification à double facteur.

➢ <u>Faiblesse</u>

L'authentification double facteurs améliore la sécurité. Mais elle n'est pas la panacée. Par exemple, un Token physique peut être compromise par une attaque contre son fournisseur comme ce fut le cas en 2011 pour RSA Security et ses tokens SecurID.

Le processus de récupération de mots de passe oubliés est également un maillon faible de cette technique. Lors du renouvellement d'un mot de passe demandé par un utilisateur qui l'aurait oublié, un nouveau mot de passe temporaire est envoyé par mail et permet de contourner la double authentification. C'est ce qui est arrivé au président de Cloudfare dont l'adresse Gmail professionnelle avait été piratée.

Autre limitation, la double authentification qui s'appuie sur les SMS – simple à mettre en place et donc populaire - n'est plus considérée comme sûre. Le National

Institute of Standards and Technology (NIST) a déprécié cette méthode dans ses Special Publication 800-63-3: Digital Authentication Guidelines. Les mots de passe temporaires envoyés par ce biais sont trop vulnérables aux attaques réseaux ou à des malwares comme Eurograbber qui peuvent intercepter et rediriger les SMS.

- Comparaison

Grâce aux différents facteurs d'authentification, des méthodes de vérifications ont été mises en place pour qualifier le degré d'authentification. C'est-à-dire que l'on peut combiner un ou deux facteurs pour renforcer la vérification. Il existe 3 familles d'authentification : simple, forte et unique.

Une authentification simple est une procédure d'authentification qui ne requiert qu'un seul facteur d'authentification. L'authentification simple la plus courante est le mot de passe. Nous n'avons eu cesse de le dire, l'authentification simple n'est pas un système fiable sachant que les méthodes de pirateries deviennent de plus en plus efficace. L'authentification unique est une méthode permettant à un utilisateur d'accéder à plusieurs applications informatiques (ou sites web sécurisés) en ne procédant qu'à une seule authentification. C'est justement ce dernier procédé que le gouvernement français a voulu soutenir via le dispositif « France Connect » permettant aux citoyens français de s'identifier sur les principaux sites publics via un seul jeu d'identifiants. Cela permet aux utilisateurs de s'identifier une seule fois, limitant ainsi les risques en réduisant le nombre de mots de passe à retenir. L'authentification forte, elle demande d'associer plusieurs preuves en vue d'effectuer cette validation, par exemple quelque chose que l'on sait (mot de passe, code PIN) avec quelque chose que l'on possède (un élément biométrique, un objet ou une action).

Partant du constat simple que le premier élément de sécurité est l'identité et que le vrai point faible de l'identité est le mot de passe, l'authentification unique apparaît également comme une bonne stratégie à adopter pour toute entreprise ou particulier souhaitant en finir avec la multiplicité des identifiants et des mots de passe tels que nous les avons connus jusqu'à présent. Cette approche fournit également une expérience utilisateur améliorée pour les employés, les clients ou les citoyens. Pourtant, elle ne résout pas seule les enjeux de sécurité associés à l'authentification. Alors que la mobilité et le Cloud font voler en éclat le périmètre de sécurité traditionnel des entreprises, celles-ci doivent s'efforcer de trouver de nouvelles stratégies pour se protéger.

De plus, les vols massifs d'identifiants et mots de passe soulignent d'autant plus le besoin de renforcer l'authentification avec plusieurs facteurs afin de limiter les risques de fraude liés à une simple authentification du couple identifiant/mot de passe. Yahoo en est à ce titre le dernier exemple de taille avec l'annonce il y a quelques jours d'un

piratage de près de 500 Millions d'identifiants et mots de passe de clients s'étant déroulé plus de 18 mois auparavant !

Le couplage de l'authentification unique à l'authentification forte rend un double service auprès des utilisateurs : d'une part le consommateur ou l'employé bénéficie d'une expérience améliorée (et d'un réel confort), et d'autre part il permet d'élever de manière très conséquente la sécurité des services rendus tout en diminuant le risque de fraude. L'avenir est à la combinaison de ces deux moyens. Les solutions de gestion des identités connaissent une adoption de plus en plus généralisée car elles proposent une expérience client homogène et répondent à des contraintes strictes en matière de sécurité, de performances et de besoins techniques. Beaucoup d'entreprises et autres organismes ont déclaré que la fin du mot de passe était proche, il faut maintenant se pencher sur ce qui vient après.

II- QUELQUES SOLUTIONS CONCERNANT LA MISE EN PLACE DES SYSTEMES A DOUBLE FACTEURS

Les enjeux pour une entreprise sont grands. En effet, toutes entreprises ou entités possèdent des données sensibles et privées. Ainsi chaque administrateur système de l'entreprise doit créer un compte personnel d'accès à chaque salarié. Les personnes externes de l'entreprise ne pourront ainsi pas accéder aux données. L'authentification forte doit être privilégiée, car les tentatives de fraudes et de vols de données contre une somme d'argent sont de plus en plus fréquentes. Par exemple, en plus d'entrer son mot de passe, il faut fournir un autre moyen d'authentification qui peut être un numéro de téléphone, une reconnaissance vocale, une image, un code alphanumérique etc.

Aujourd'hui, les entreprises ne doivent en aucun cas faire l'impasse sur les solutions de protection des données et de gestion d'identité des utilisateurs au risque de voir ses données en danger et/ou être dérobées.

La technologie d'authentification forte peut être mise en place pour tout type de système. Même s'il présente une architecture quelque peu plus complexe et lourde que la méthode traditionnelle, ces moyens et outils dépendent les informations à protéger. En outre, dans l'authentification forte on s'associe le mot de passe (facteur mémoriel) à un autre moyen d'authentification. Ainsi il serait judicieux de baser la deuxième authentification sur un autre type de facteur.

La liste suivante fait mention de quelques solutions qui peuvent être mis en place dans un système local :

Accès par puces RFID couplé à un mot de passe

Cette technique est semblable à l'authentification qu'offrent les banques en ce qui concerne les cartes magnétiques et les comptes bancaires. Il est possible de les appliquer pour l'accès aux datacenters d'une IT entreprise. On pourra utiliser la technologie NFC.

Accès avec des systèmes biométriques couplé à un mot de

passe. One Time Password + Mot de passe traditionnel

Ici on a la possibilité d'utiliser ce système sur les applications et sites web. Spécifiquement, on utilise le temps et la date pour fournir un code qui sera éventuellement par mail ou par SMS. Ainsi l'utilisateur en plus d'entrer son login et son mot de passe, il y ajoutera un code externe pour corser l'usurpation. Toujours dans la même veine on a MultiOTP de SysCo systèmes de communication sa, une classe PHP libre incluant un outil en ligne de commande pour fournir une solution d'authentification forte indépendante de tout système d'exploitation.

Google Authentificator : est un API ge Google, qui de finir une authentification double facteur au niveau des smartphones Android et IPhone.

Ainsi la deuxième authentification se présente comme une fenêtre accueillant le nouveau code ou juste un bouton de confirmation.

OpenOTP de RCDevs, une solution fonctionnant sous différentes distributions de Linux

III- EXEMPLE D'AUTHENTIFICATION A DOUBLE FACTEURS

Pour notre cas nous avons choisi de présenter l'authentification à double facteurs de Google.

L'authentification à double facteur avec Google peut se faire de plusieurs manières. La méthode d'activation diffère selon l'appareil utiliser (un ordinateur, sur un smartphone ou sur un IOS). Pour notre exposé nous allons montrer comment l'activer sur ordinateur et sur un Android.

Configuration sur Smartphone

Pour Android allez dans paramètres dans l'option Google puis dans compte Google puis dans sécurité activer la validation en deux étapes. Et vous suivez les instructions.

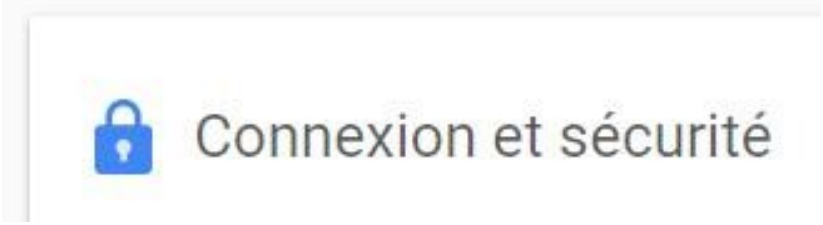
NB : Pour les options de connexion à votre compte en cas de perte de téléphone, Google vous propose d'entrer un numéro secours ou encore il vous génère une série de code que vous pouvez utiliser pour vous connectes sur d'autres téléphone.

Configuration sur ordinateur

Vous vous connecter à votre compte Gmail rendez-vous dans l'onglet mon compte en haut à droite en cliquant sur la partie photo de profil.

Ensuite vous cliquer sur mon compte :

Ensuite vous allez dans la partie connexion et sécurité :



Dans la partie se connecter à Google, on vous propose le service. Vous avez juste à cliquer sur démarrer à droite.

- Cliquer sur **configurer**.

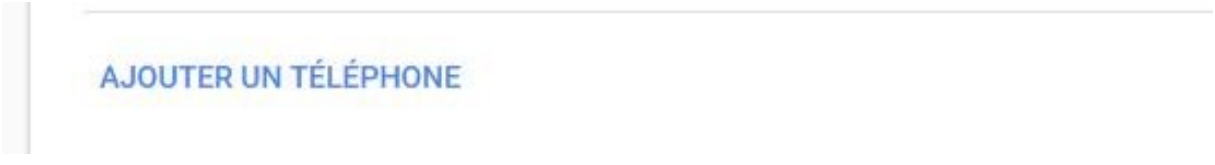
Google vous demande d'entrer votre mot de passe ensuite un téléphone qui vous aidera à vous connecter.

- Vous cliquez sur **suivant** et vous confirmer votre adresse email.

Ensuite une configuration vous serra demande sur le téléphone en question.

- Dernière ligne droite vous cliquer sur **activer** et **Bravo**.

Google vous donne la possibilité d'ajouter d'autre portable pour vous connecter.



Désormais pour vous pouvez-vous connecter à votre compte Gmail à l'aide de votre téléphone. Une autre application que vous pouvez utiliser dans le cas des authentifications doubles facteurs est Google authentificator.

Alors qu'est-ce que Google authentificator ?

Google Authentificator est un logiciel open source développé par Google qui permet la gestion des connexions à des comptes sur le web. Vous pouvez télécharger gratuitement l'application sur **play store** pour Android.

Principe de fonctionnement

Le principe de fonctionnement de Google Authentificator est simple.

Il faut scanner le QR code affiché sur le site web avec de l'application installé sur votre smartphone. Il faut ensuite entrer un code à 6 chiffres généré par l'application pour vérifier l'association avec le compte. Une fois configuré, à chaque fois que vous essayerez de vous connecter à votre compte Google sur une machine inconnue, le service demandera de rentrer un code à 6 chiffre générés par l'application, après l'étape de de saisi du mot de passe.

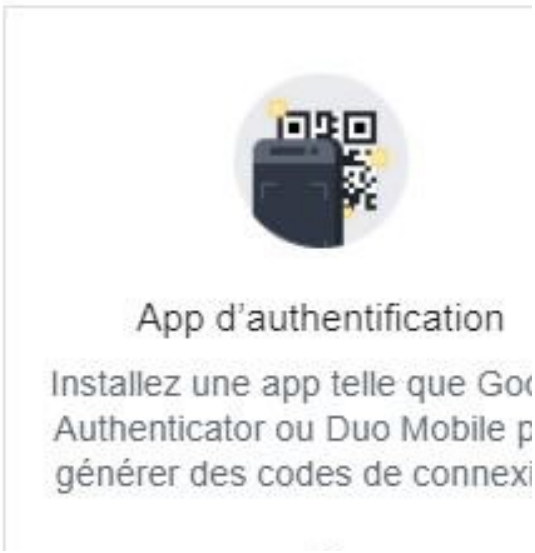
Notez que l'application Google Authenticator utilise l'algorithme TOTP implémenté par de nombreux services sur le web. **L'application pourra donc servir pour beaucoup d'autres comptes sur le web** chez différents fournisseurs de service. La procédure est d'ailleurs souvent la même : se rendre dans les paramètres de sécurité du compte, trouver l'option, scanner un QR Code et rentrer un code à 6 chiffres. L'application génère le code de 6 chiffres chaque 1 minute. Pour changer un peu d'environnement. Nous allons faire ce test avec Facebook.

Utilisation de Google Authentificator avec Facebook

- Lorsque vous êtes connecté à votre compte Facebook, allez dans les paramètres ensuite dans connexion et sécurité.

- Vous allez dans authentification à deux facteurs

- Ensuite vous cliquer sur démarrer
- Vous choisissez l'option App d'authentification.



Ensuite vous cliquez sur suivante. Maintenant Google authentification intervient. Nous allons scanner le QR code avec l'application Google Authentificator.

Apres cette étapes notre application va prendre en compte notre compte Facebook et généra un code de 6 chiffres compte chaque une minute.

NB : Pour chaque connexion sur un appareil qui n'a pas été pris en compte Facebook demandera ce code de 6 chiffres. Vous avez la possibilité de confirme.

CONCLUSION

En conclusion, nous pouvons dire que l'authentification à double facteurs vient augmenter de manière considérable la sécurité des systèmes. Les entreprises implémentent au fur et à mesure cette solution, qui peut s'appliquer sur tout type d'architecture. Mais la sécurité n'était jamais absolue, on veut observer certaines faiblesses au niveau de l'authentification à double facteurs. Ces faiblesses peuvent se situent au niveau des outils des technologies utilisées ou même encore du manque de maturité sécuritaire de certains utilisateurs. On pense désormais à des systèmes d'authentification à trois facteurs qui influerait une entité tiers pour le processus de validation de l'identité.