Thomas Pélissier

Naoual Mouzouri

Karim Jebara

Master 2 MIAGE

Solutions matérielles de double authentification

Monsieur Courtaud

2015/2016

Table des matières

Introduction

La démocratisation de l'utilisation d'internet a conduit les entreprises à ouvrir leurs systèmes d'informations aussi bien que pour leurs clients, partenaires et fournisseurs. La question de la sécurité se pose alors pour les entreprises.

Il est absolument nécessaire pour ces dernières, de définir toutes leurs ressources sensibles afin de les protéger, et maîtriser le contrôle d'accès à ces informations. Pour cela, elle doit en amont mettre en place une solution de droits des utilisateurs sur son système d'information.

Cette politique de droits doit par la suite être étendue lors de l'ouverture du système d'information avec l'extérieur par le biais d'internet.

Plus récemment, l'apparition des ordinateurs portables ont conduit les entreprises à sécuriser l'ensemble de leur infrastructure informatique. Dans le cas où l'ordinateur portable d'un collaborateur de la société venait à tomber dans les mains d'un concurrent ou d'une personne malveillante, si ce dernier n'est pas sécurisé, toutes les informations seront visibles par cet individu.
On peut facilement imaginer les conséquences néfastes pour l'entreprise.

1. La sécurité informatique

1.1 Définition

Toute entreprise dispose à ce jour d'un système informatique [1]. Celui-ci permet de collecter, stocker, traiter et diffuser des informations dans l'objectif de répondre aux besoins de la société.

Comme énoncé dans l'introduction, le système informatique d'une entreprise est vulnérable depuis l'extérieur par le biais d'internet mais il l'est également depuis l'intérieur.

La sécurité informatique [2], par définition, permet de sécuriser un système informatique. L'objectif étant de limiter au maximum le risque[1] de menace[2] d'attaque, dans ce cas le système est vulnérable[3]. Afin de prévenir la menace, une entreprise doit mettre en place un ensemble de contre-mesures[4] [3].

Les entreprises appliquent deux types de contre-mesures [4] :

- mettre en place des procédures afin de sécuriser l'infrastructure informatique,
- former et sensibiliser les collaborateurs sur les menaces.

Dans l'optique de sécuriser son système informatique, l'entreprise se doit en amont d'identifier les menaces possibles. En fonction de cette identification, elle doit mettre en place les contre-mesures nécessaires.

[1] On définit le risque par l'équation suivante : Risque = (Menace X Vulnérabilité) / (Contre-Mesure)
[2] La menace représente une action capable de nuire à l'activité de l'entreprise.
[3] La vulnérabilité est le niveau d'exposition face à la menace d'un système informatique.
[4] La contre-mesure est l'ensemble des actions mises en œuvre en prévention de la menace.

1.2 Finalité de la sécurité informatique

L'objectif de la sécurité informatique est d'assurer que les ressources aussi bien matérielles que logicielles sont employées uniquement dans l'entreprise et le cadre de son cœur de métier [5]. Elle permet de protéger le patrimoine de cette dernière.

La sécurité informatique permet de répondre aux objectifs suivants :

- la disponibilité : l'entreprise doit définir le moment de la journée ou les informations doivent être impérativement disponibles. Certaines informations devront être disponibles pendant le temps de travail, d'autres toute la journée. Une fois cette définition réalisée, le système doit fonctionner sans faille durant les plages d'utilisation prévues et ainsi garantir l'accès aux services et ressources installées avec le temps de réponse attendu ;

- l'intégrité : le traitement, la conservation et la transmission des données ne doivent subir aucune destruction volontaire, accidentelle et aucune altération ;

- la confidentialité : seules les personnes autorisées ont accès aux informations qui leurs sont destinées. Tout accès indésirable doit être empêché ;

- la traçabilité : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables ;

- l'authentification : l'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange ;

- la non-répudiation : aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

1.3 Démarche à entreprendre

La démarche générale pour l'entreprise consistant à mettre en place une sécurité du système d'information est la suivante [6] :

1) Définir et évaluer les risques et leur criticité[5]. C'est-à-dire, en fonction de chaque type de donnée définir quels sont les risques, les menaces et quelles sont les conséquences en cas de pertes de cette donnée.

2) Déterminer et adopter les contre-mesures à mettre en place. On doit se poser la question que doit-on sécuriser et comment.

3) Appliquer et tester les contre-mesures misent en place.

[5] La criticité est la détermination et hiérarchisation du degré d'importance et de la disponibilité du système d'information.

Une fois les contre-mesures misent en place, cela ne suffit pas pour garantir une sécurité du système. Il faut impérativement vérifier régulièrement les contre-mesures en réalisant des tests, s'adapter en fonction des nouvelles méthodes d'attaques.

1.4 Identification des menaces

Quatre sources de menaces ont été caractérisées :

1) L'entreprise peut être soumise à un endommagement de matériel informatique dû à un sinistre (vol, incendie, dégât des eaux, …). Dans ce type de situation, les données sont généralement perdues.

2) Un utilisateur du système d'information peut mettre en péril intentionnellement ou non, la sécurité du système d'information.

3) Un programme malveillant installé par un utilisateur du système par mégarde ou non, peut conduire à créer des failles de sécurité dans le système.

4) Une personne extérieur (hacker) à l'entreprise qui parvient à percer toutes les protections du système et arrive par conséquent à s'y introduire et avoir accès aux données.

1.5 Identification des dommages

Il existe quatre types de dommages que peut rencontrer une entreprise en cas de manquement en termes de sécurité de son système d'information :

1) Des dommages de types financiers :
    1.1 Soit sous forme de coûts directs, c'est-à-dire le remplacement de matériels suite à un sinistre, la reconstitution de données perdues, …
    1.2 Soit sous forme de coûts indirects, c'est-à-dire le vol d'un secret de fabrication, de plan stratégique d'investissement futur …

2) Suite à une attaque, l'image de marque de l'entreprise sera affaiblie.
    2.1 Affaiblissement direct suite à une publicité négative faite par la publication de l'attaque.
    2.2 Affaiblissement indirecte par la baisse, voire la perte de confiance des consommateurs.

3) Des dommages par non-respect légale de la disponibilité des données. L'indisponibilité d'un système d'information peut conduire l'entreprise à une situation de défaut face à ses obligations légales et juridiques.

4) Des dommages écologiques et sanitaires : une panne du système d'information peut conduire à des catastrophes écologies et/ou sanitaires.

Afin de protéger au mieux les systèmes d'informations, nous allons nous intéresser aux fonctionnements de deux nouvelles technologies de sécurité : FIDO et U2F.

2. FIDO (Fast ID Online)

2.1 Présentation

FIGURE 1 : REPRESENTATION DU LOGO FIDO

FIDO [7] (Fast ID Online) est un ensemble de spécifications de sécurité technologique agnostique pour l'authentification forte. FIDO est développé par FIDO Alliance, un organisme sans but lucratif formé en 2012.

La spécification FIDO admet l'authentification multifactorielle (AMF) et la cryptographie avec clé publique. Un avantage majeur de l'authentification FIDO est le fait que les utilisateurs ne doivent pas utiliser de mot de passe complexe, traitant avec les règles de mot de passe fort complexent et/ou passent par des procédures de récupération quand ils oublient un mot de passe.

Contrairement à des bases de données de mots de passe, les bases de données FIDO-informations ont une identification personnelle (PII) telles que les données d'authentification biométriques qui sont sur les périphériques utilisateur pour le protéger. Le stockage local FIDO de la biométrie et autre identification personnelle est destiné à alléger les préoccupations des utilisateurs sur leurs données personnelles stockées sur un serveur externe dans le Cloud. En faisant abstraction à la mise en œuvre du protocole d'interfaces de programmation d'application (API), FIDO réduit également le travail requis pour les développeurs de créer des connexions sécurisées pour les clients mobiles fonctionnant sous différents systèmes d'exploitation (OSE) et sur différents types de matériel.

FIDO supporte le Framework universel d'Authentification (UAF) ainsi que le protocole U2F (Universal second factor). Avec UAF, le dispositif client crée une nouvelle paire de clés lors de l'inscription à un service en ligne et conserve la clé privée ; la clé publique est inscrite sur le service en ligne. Lors de l'authentification, le dispositif de client entre en possession de la clé privée pour le service en signant une preuve, ce qui implique une action physique comme fournir une empreinte digitale, la saisie d'un code PIN ou en parlant dans un microphone. Avec U2F, l'authentification requiert un deuxième facteur clé qui est le Near Field Communication (NFC) ou le jeton de sécurité.

2.2 Historique

En 2007, PayPal a essayé d'augmenter la sécurité en introduisant AMF à ses clients sous la forme de son mot de passe à usage unique (OTP) porte-clés : clé sécurisée. Bien que Secure Key fût efficace, les taux d'adoption étaient bas. Il est généralement utilisé que par quelques individus soucieux de la sécurité. Les porte- clés d'authentification sont complexes, et la plupart des utilisateurs ne sentaient pas le besoin de l'utiliser.

Dans les discussions qui explorent l'idée d'intégrer la technologie de « fingerscanning » à PayPal, Ramesh Kesanupalli (directeur technique de capteurs de validité) a parlé à Michael Barrett (CISCO puis de PayPal). Barrett soutenait l'avis qu'un standard de l'industrie était nécessaire par le soutien du matériel d'authentification. Kesanupalli partit de là pour rassembler les pairs de l'industrie avec cette fin à l'esprit.

L'Alliance a été fondée par FIDO à la suite de réunions entre le groupe. L'Alliance est devenue publique en Février 2013 et depuis ce temps, de nombreuses entreprises sont devenues membres, y compris Google, ARM, Bank of America, Master Card, Visa, Microsoft, Samsung, LG, Dell et RSA.

Microsoft a annoncé l'inclusion de FIDO pour l'authentification dans Windows 10

2.3 Le fonctionnement interne FIDO

Comme évoqué dans l'introduction [8], FIDO est un ensemble de protocoles qui sont utilisées en vue de garantir une authentification forte grâce notamment à des standards de cryptographie à clé publique.

Lorsqu'un utilisateur va s'inscrire sur une application en ligne, l'ordinateur de l'utilisateur va créer une nouvelle paire de clés. Pendant le processus d'inscription, l'utilisateur devra fournir la clé publique au serveur de l'application et conserver sa clé privée.

Le dispositif physique du client va permettre de prouver qu'il est bien en possession du dispositif physique et donc de la clé privée. En interagissant avec ce dispositif, l'utilisateur va pouvoir s'authentifier sur le serveur de l'application car ce dispositif lui sert de preuve. La clé privée de l'utilisateur est présente sur le dispositif, sans lui, après avoir réalisé l'étape d'inscription, il ne pourrait pas s'authentifier.

Afin de déverrouiller le dispositif de manière sécurisée, généralement l'utilisateur doit simplement appuyer sur un bouton. D'autres dispositifs incluent les possibilités de reconnaitre les données biométriques d'un doigt ou de notre voix. Ce type de dispositif est plus rare et beaucoup plus cher à l'acquisition dû à leur complexité.

Les protocoles FIDO ont était conçus dans l'optique de protéger les données et la vie privée des utilisateurs. Le très grand avantage de l'utilisation de ces protocoles et la sécurité des messages échangés entre le dispositif de l'utilisateur et le serveur de l'application.
En effet, il est impossible, en cas d'interception d'un message de pouvoir décrypter la clé privée du dispositif et par conséquent il est impossible de récupérer des informations sur le détenteur du dispositif.

Ainsi, quand bien même un message serait intercepté par une personne malveillante, ou bien que le serveur d'une application soit piraté, il est impossible de pouvoir s'authentifier en se passant pour cet utilisateur sur d'autres applications. [9]

2.4 Le fonctionnement de l'enregistrement sur une application en ligne

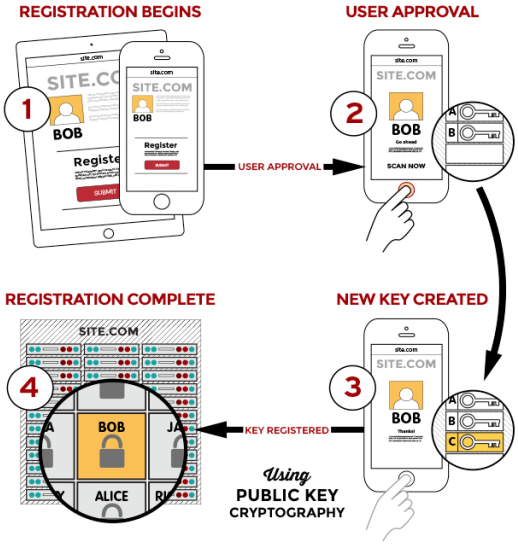

FIGURE 2 : PROCESSUS D'INSCRIPTION EN LIGNE AVEC FIDO

1) L'utilisateur est invité à choisir un authentificateur FIDO disponible qui correspond à la politique d'acceptation des services en ligne.

2) L'utilisateur déverrouille l'authentificateur FIDO à l'aide d'un capteur d'empreintes digitales. Dans cet exemple, le dispositif est un smartphone de dernière génération. Une autre méthode aurait consisté à appuyer sur le bouton d'un dispositif pour déverrouiller l'authentificateur FIDO.

3) Le dispositif de l'utilisateur crée une nouvelle paire de clés publique / privées à usage unique. Cette double paire de clés va permettre d'enregistrer l'utilisateur pour la première fois. La clé privée va rester en local au sein du dispositif alors que la clé publique sera envoyée au serveur de l'application en ligne.

4) Par la suite, la clé publique est envoyée au serveur de l'application en ligne et associée au compte utilisateur. Uniquement la clé publique et le compte utilisateur sont envoyés au serveur. Les informations biométriques par exemple restent conservées au sein du dispositif.

2.5 Le fonctionnement de l'authentification sur une application en ligne

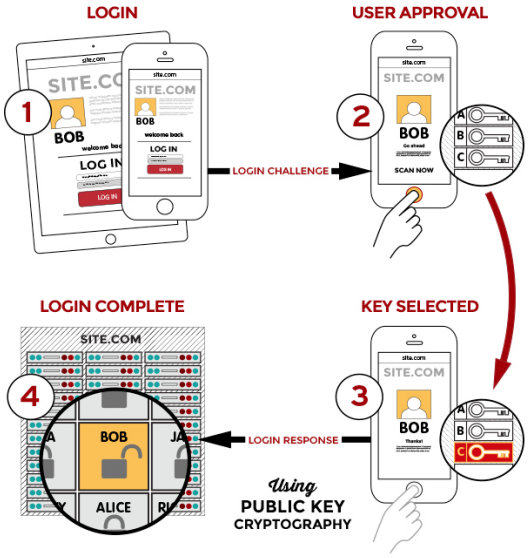

FIGURE 3 : PROCESSUS D'AUTHENTIFICATION EN LIGNE AVEC FIDO

1) L'application en ligne demande à l'utilisateur de bien vouloir s'authentifier par le biais d'un dispositif déjà inscrit en ligne.

2) L'utilisateur déverrouille l'authentificateur FIDO en utilisant la même méthode que lors de l'inscription sur l'application.

3) Le dispositif physique se fait passer pour votre compte utilisateur une fois que le serveur a reconnu la bonne clé et la preuve fournit par le dispositif.

4) Le dispositif physique de l'utilisateur envoi la preuve vers le serveur de l'application, ce dernier vérifie avec la clé et les logs de l'utilisateur que c'est bien lui avant de l'authentifier.

3. U2F (Universal 2nd Factor)

3.1 Présentation

FIGURE 4 : REPRESENTATION DU LOGO U2F

U2F [10] est un standard d'authentification ouvert qui permet aux internautes d'accéder en toute sécurité à un certain nombre de services en ligne, avec l'aide d'un appareil, instantanément et sans aucun pilote ou logiciel client nécessaires.

U2F a été créé par Google et Yubico, avec la contribution de NXP, et est aujourd'hui hébergé par le consortium d'industrie d'authentification ouverte FIDO Alliance.

Les spécifications techniques ont été lancées à la fin 2014, y compris le support natif dans les comptes Google et Chrome, et ont depuis donné lieu à un écosystème florissant de fournisseur de matériel, de logiciels et de services.

Le protocole d'U2F a franchi une étape importante en juin 2015, l'ajout de nouveaux protocoles de transport de message qui s'adresse aux appareils mobiles.
U2F fonctionne sur les appareils mobiles qui utilise la technologie NFC – Google authenticator v4.44 et GitHub ont tous les deux déployé le nouveau protocole de transport en Décembre 2015.

3.2 Les apports cette nouvelle technologie

Les intérêts d'utiliser cette nouvelle technologie U2F sont multiples. Grâce à la mise en place d'un système U2F les utilisateurs pourront bénéficier de différents avantages :

Une sécurité renforcée : une authentification forte avec la présence de deux facteurs, en utilisant une clé cryptée publique et avec un support natif dans le navigateur (sur Chrome notamment). Ceci va également permettre de lutter face au « phishing », au détournement de session (hacking), des attaques de type « man in the middle », et également les attaques de malware.

Facile à utiliser : possibilité de s'authentifier instantanément à un certain nombre de services. Aucun code n'est nécessaire ni même de pilote à installer.

Données privées : permet aux utilisateurs de choisir, d'obtenir et de contrôler la sécurité de leur identité en ligne. Chaque utilisateur peut également choisir d'avoir plusieurs identités, y compris des identités anonymes (pas d'informations personnelles associées à l'identité de l'utilisateur). Le dispositif d'U2F génère une nouvelle paire de clés pour chaque service, la clé publique est stockée uniquement sur le service spécifique. Avec cette nouvelle approche, aucune donnée visible n'est partagée entre le fournisseur du service et l'utilisateur.

Un choix multiple : conçu pour des téléphones et ordinateurs actuels, pour de nombreuses modalités d'authentification (par exemple des smartphones, des porte-clés, des lecteurs d'empreintes digitales, etc…) et comprenant de nombreuses méthodes de communication (USB, NFC, Bluetooth).

Interopérable : des standards ouverts soutenus par des services financiers et de l'internet, notamment Google, Bank of America et 250 entreprises du consortium de l'Alliance FIDO. U2F permet à chaque fournisseur de services d'être également leurs propres fournisseurs d'identités, ou éventuellement permettre aux utilisateurs authentifiés par un fournisseur de services fédérés.

Rentable : les fournisseurs de services ne doivent pas prendre le coût et le support de la distribution du dispositif sécurisée d'U2F. Les utilisateurs peuvent choisir parmi une gamme d'appareils à faible coût provenant de plusieurs fournisseurs, disponible notamment via la plateforme Amazon et d'autres magasins de détail à travers le monde. Yubico propose un logiciel gratuit d'open source d'intégration.

Identité électronique : Pour les services nécessitant un niveau plus élevé d'identité assuré, les services sont actuellement en cours d'élaboration, à la fois en ligne et dans le monde physique, pour rattacher votre appareil U2F à votre véritable identité.

Récupération sécurisée : il est recommandé que les utilisateurs enregistrent au moins deux dispositifs de type U2F à chaque fournisseur de services, ce qui peut éventuellement fournir à l'utilisateur un code de sauvegarde au cas où un dispositif U2F était défectueux.

3.3 Fonctionnement d'un dispositif U2F

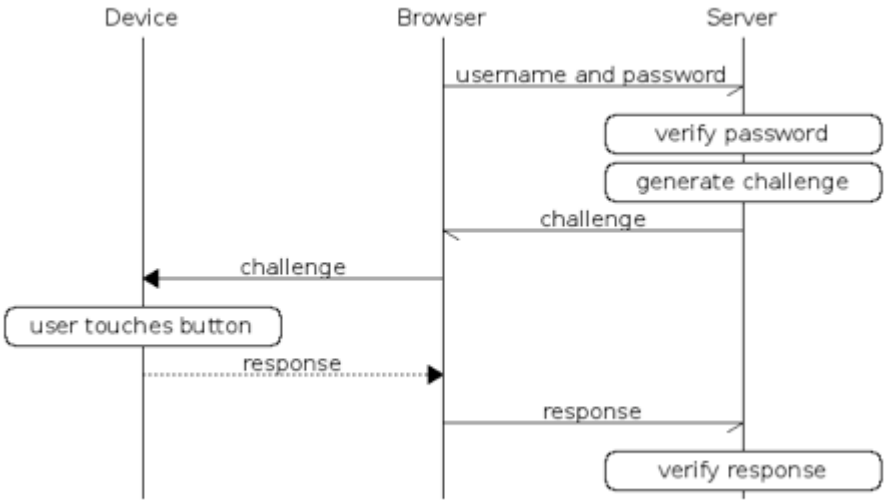

FIGURE 5 : REPRESENTATION DES ECHANGES D'UN DISPOSITIF U2F

Dans un premier temps, le navigateur va transmettre les informations nécessaires à l'authentification d'un utilisateur (à savoir son mot de passe et son nom d'utilisateur) au serveur.

Le serveur va vérifier le mot de passe et va ensuite générer une demande de preuve de véracité de l'identité de l'utilisateur.

Le serveur va envoyer cette demande de preuve au navigateur qui lui va la transmettre au dispositif U2F.
Dans ce cas, l'utilisateur sera averti qu'il doit appuyer sur le bouton du dispositif présent dans son port USB.

Le dispositif U2F va transmettre son code d'authentification au Navigateur qui lui va la transmettre au Serveur.

Enfin le serveur va vérifier le code de cette réponse et l'utilisateur sera à ce moment-là totalement authentifié et de manière sécurisé.

3.4 L'attestation d'U2F

Le but de l'attestation d'U2F est simplement de fournir un mécanisme de sorte qu'une partie utilisatrice d'U2F (un site web ou un service) peut vérifier l'authenticité d'un authentificateur U2F et ainsi la confiance à son certificat d'attestation d'authenticité.

La partie qui interroge le certificat d'attestation invoque de trouver des informations sur un authentificateur, tel que YubiKey. Les informations demandées peuvent inclure le vendeur, le type d'appareil, et les propriétés de sécurités (par exemple un dispositif à base d'élément sécurisé) de l'authentificateur. L'authenticité de l'information d'attestation est garantie par une signature numérique qui a une durée de validité spécifiée.

En complément de l'attestation de l'authenticité d'un dispositif, le certificat d'attestation peut aussi être utilisé pour déterminer quels appareils peuvent être utilisés par une partie de confiance.
Par exemple, dans le cas d'un site bancaire qui voudrait que leurs clients soient en mesure de fournir leurs propres dispositifs U2F pour les authentifiés sur leur serveur.

Il n'existe pas de condition, le service peut accepter tout type de certificat d'attestation ou de type spécifique.

Conclusion FIDO et U2F

FIDO est un protocole qui permet d'authentifier un utilisateur sur une application en ligne via une solution complémentaire du traditionnel compte utilisateur et mot de passe.

FIDO dispose de deux méthodes d'authentification possible : UAF et U2F :

- Dans le cas UAF : FIDO est pris en charge par le protocole UAF (Universal Authentification Framework). Un utilisateur s'enregistre et s'authentifie sur le serveur d'une application en ligne en choisissant un dispositif d'authentification local, comme saisir un code PIN, glisser son doigt dans un lecteur biométrique, regarder une caméra, parler dans un micro. Une clé privée est créée par le dispositif UAF et stockée sur l'appareil, la clé publique est générée et transmise au serveur en ligne.

- Dans le cas U2F : un dispositif permet de sécuriser d'avantage les infrastructures, en effet un second facteur (le Near Field Communication (NFC) ou le jeton de sécurité) est ajouté en plus de l'identification réalisée avec les clés privées et publiques du système UAF. Comme par exemple l'ajout d'un dispositif de type YubiKey dans le processus d'authentification. Ce moyen d'authentification est ultra-sécurisé comparé à UAF. [11]

4. Fonctionnement de l'authentification sans mot de passe (YubiKey)

4.1 Introduction

L'authentification a pour but de donner l'accès à une ressource protégée en vérifiant par une manière donnée que l'utilisateur qui cherche à obtenir l'accès à cette ressource soit bien la personne qu'elle prétend être.

Pour cela à ce jour les manières les plus répandues sont l'utilisation d'une double authentification avec le nom de l'utilisateur ainsi que son mot de passe. Ainsi on identifie en théorie une personne avec deux éléments que celle cette personne est sensée connaitre.
Cependant, on s'est aperçu qu'aujourd'hui des nouvelles méthodes permettaient « facilement » d'usurper l'identité d'un individu. Notamment avec des méthodes de « phishing », « man in the middle », etc.

Pour pallier à cette faille de sécurité, l'avenir prévoit une nouvelle méthode d'authentification. Toujours grâce à la combinaison du nom d'utilisateur et mot de passe mais également avec l'apparition

d'un dispositif physique. Ainsi, on ne pourra non plus authentifier un utilisateur par ce qu'il connait (son mot de passe et son nom d'utilisateur) mais par ce qu'il détient.

Grâce à cette nouvelle combinaison, nous avons la certitude que l'utilisateur est bien l'unique détenteur de son identité virtuelle.

4.2 Les difficultés de conception

La difficulté de conception de ces nouveaux outils repose sur le facteur suivant : Comment trouver une méthode qui permet de prouver que l'utilisateur est bien le détenteur de l'objet à l'instant où il réalise l'authentification.

Au tout début, des « cryptologues » pensaient qu'il suffisait « simplement » d'attribuer un identifiant supplémentaire lors de l'authentification. Par exemple saisir le numéro de série d'un appareil. Cependant ils se sont très vite aperçu que le problème n'était pas résolu, qu'on pouvait très facilement récupérer ce numéro de série pour usurper l'identité d'un utilisateur.

En effet, on ne peut évidemment pas se baser sur une méthode aussi simple qu'un numéro de série inscrit sur l'objet, puisqu'il suffirait de récupérer ce numéro une seule fois pour pouvoir s'authentifier sans avoir réellement l'objet avec soi.

Par la suite des véritables cryptologues se sont penchés sur le sujet. Ils en sont venus à concevoir plusieurs méthodes d'authentifications. La plupart de ces systèmes d'authentification repose sur une méthode de clés de chiffrement (symétrique ou asymétrique) dont notamment la clé privée va être écrite uniquement sur l'objet.

Ainsi, grâce à cette méthode, personne ne pourra donc jamais avoir accès à ce numéro si ce n'est le fabriquant de l'objet, généralement l'utilisateur n'y a pas accès sauf si ce dernier parvient à accéder à cette clé, chose très complexe.

4.3 Les différentes solutions de chiffrement

4.3.1 La YubiKey

A ce jour, il semblerait que d'après les avis des utilisateurs et des entreprises, la clé YubiKey [12] développée par la société Yubico soit la clé physique la plus simple d'utilisation à ce jour.

FIGURE 6 : REPRESENTATION DE LA CLE YUBIKEY4

La clé YubiKey est une petite clé USB qui simule dans l'ordinateur un clavier de type USB. Au sein de la YubiKey se trouve une clé AES en écriture seule (c'est-à-dire qu'il est impossible de lire le contenue de la clé).

4.3.1.1 Le fonctionnement interne de la YubiKey

À chaque appui sur le bouton présent sur la clé, la YubiKey va émettre une chaine composée de son identifiant ainsi qu'un compteur de session. C'est-à-dire que chaque fois que l'on va brancher notre clé à notre port USB, un compteur va s'incrémenter.

Il y a également au sein de cette YubiKey un compteur « d'horloge ». C'est-à-dire que d'après la documentation technique disponible sur le site de Yubico, ce compteur d'horloge va s'incrémenter avec la caractéristique suivante : incrémentation de 8 toutes les secondes.

Enfin, un compteur d'utilisation de la clé est intégré dans la YubiKey. Chaque fois que l'utilisateur appui sur le bouton de la clé, alors le compteur s'incrémente.

Toutes ces informations sont envoyées sous forme de chaine chiffrée avec la clé interne AES au serveur qui cherche à nous authentifier et sur lequel on s'est déjà inscrit au préalable avec cette clé.

Donc la YubiKey possède plusieurs informations qui évoluent au cours de son utilisation qui la rend quasiment inviolable :

- Un compteur de session
- Un compteur d'horloge
- Un compteur d'utilisation
- Une clé AES interne

4.3.1.2 Les données échangées avec la YubiKey

Lorsque l'utilisateur s'identifie sur une application, site web qui supporte la technologie de la YubiKey voici comment va réagir la clé et l'application :

1) L'utilisateur saisit ces identifiants (mot de passe et nom d'utilisateur) et il appuie sur le bouton de la YubiKey.
2) Le site web va recevoir ces informations et va les envoyer sur le serveur de Yubico pour vérification sous forme de chaine chiffrée.
3) Le serveur de Yubico possède la clé privée de la clé et il est capable de déchiffrer les données et de les vérifier.
4) Si le serveur valide la véracité des informations (valeurs de tous les compteurs), dans ce cas il renvoie au serveur du site web (via un chiffrement asymétrique) un message affirmant les informations reçues par ce dernier et ainsi l'utilisateur est authentifié.

Sinon :

4 bis) Si les valeurs des compteurs sont bien strictement supérieures à celles de la dernière chaîne validée, alors cela signifie qu'il y a eu usurpation de l'identité et dans ce cas la requête de l'utilisateur est rejetée.

4.3.1.3 La sécurité de la YubiKey

L'étape de vérification des compteurs est véritablement un gage de sécurité dans l'utilisation de la YubiKey.

Prenons un exemple :

Un individu parvient à vous subtiliser votre clé YubiKey et arrive à lui faire générer des millions de chaînes. Par la suite, il repose votre clé sans que vous vous en soyez rendu compte.
Lorsque vous allez réutiliser votre clé, cette nouvelle utilisation de la clé va invalider l'intégralité de toutes les dernières chaînes enregistrées (compteur de session ou d'utilisation inférieur au compteur de la clé).

Par la suite l'utilisateur pourra réutiliser sa clé normalement.

4.3.1.4 Les avantages de l'utilisation de la YubiKey

1) Le haut niveau de sécurité de la YubiKey, en effet comme en témoigne la partie ci-dessus.

2) De nombreuses applications sont compatibles avec la Yubikey c'est le cas notamment de GitHub, Dropbox, WordPress, PAM, LUKS, OwnCloud, RoundCube, Drupal et bien d'autres en cours d'implémentation.

3) De nombreux logiciels nécessaires à l'intégration de votre YubiKey sur votre système d'exploitation sont accessibles gratuitement et sont intégrés nativement à la plupart des distributions GNU / Linux.
   Il est même possible, en vous renseignant sur les documentations présentes sur le site de Yubico de monter votre propre serveur de validation si vous ne voulez plus être dépendant de celui de Yubico.
   Cependant à ce jour, très peu d'applications supportent ce type de serveur « personnalisé » notamment GitHub, DropBox.

4) Un autre avantage est celui de la présence du double slot sur la configuration de la YubiKey. En effet, d'après les caractéristiques de la YubiKey, celle-ci dispose de 2 entrées en interne, le slot1 permet d'être appelé via un appui court sur le bouton de la clé et le slot2 par un appui long. L'intérêt est donc de pouvoir utiliser soit le serveur de Yubico soit votre serveur personnel. Il est même possible d'utiliser une clé Yubico et un mot de passe de 64 caractères aléatoires.

5) Le prix de la YubiKey, en effet, ce dispositif coûte environs une vingtaine d'euros. Ceci en fait un dispositif d'authentification très abordable.

Il existe quelques inconvénients aujourd'hui à l'utilisation de cette clé :

1) Etant donné que la clé une fois configurée sur votre ordinateur est reconnue comme étant un clavier USB, il peut arriver qu'il existe un conflit entre votre clavier USB et votre clé. Ainsi dans

des cas d'utilisation de clavier spécifique, la clé n'est pas utilisable tant que le clavier et branché et réciproquement.

2) Encore beaucoup d'applications doivent pouvoir intégrer ce système d'authentification pour que l'utilisation de la clé YubiKey puisse être véritablement une alternative incontournable au quotidien.

Il est fort à parier que la YubiKey dans les mois à venir continue à prendre de l'ampleur face aux différents cas de problème de sécurité que nous connaissons actuellement.

Dans la continuité de ce rapport, nous avons décidé de procéder à une petite étude de marché. Nous avons réalisé une mise à comparaison des solutions pouvant répondre à un haut niveau d'authentification et qui sont disponibles à ce jour. Ceci dans le but d'aider les utilisateurs soucieux de protéger leurs données.

Plusieurs solutions peuvent apporter aujourd'hui une véritable plus-value dans leur utilisation :

- Deux solutions embarquant la technologie TOTP / HOTP. Ces deux solutions peuvent être comparées avec la clé YubiKey
- La norme X.509
- Les données biométriques

Il est fort à parier qu'avec les récents problèmes de sécurités exposées par les affaires notamment d'Edward Snowden, les actions des Anonymous, etc… Les entreprises tout comme les particuliers et les développeurs décident petit à petit de sécuriser leurs données en passant notamment par des solutions exposées ci-après.

4.3.2 La solution TOTP / HOTP

La société FTSafe a mis au point une autre solution basée sur un dispositif physique dédié dénommé les OTP c100 et c200. [13]

FIGURE 7 : REPRESENTATION DES OTP C100 ET C200

4.3.2.1 Le fonctionnement interne

Le principe de fonctionnement est le même que pour les produits YubiKey. À savoir une clé privée est intégrée à l'intérieur du dispositif et l'utilisateur ne peut la modifier.
A la différence de la Yubikey, ici l'utilisateur connait sa clé privée dès lors qu'il achète le dispositif.

Lorsque l'on appuie sur le bouton de notre OTP C100 et C200, l'écran affiche un code à 6 chiffres. Ce code est calculé à partir de la clé privée ainsi que d'un compteur. Il existe deux types de compteurs un compteur de type HOTP ou un compteur de type TOTP.

Dans le cas d'un compteur de type HOTP, chaque appui sur le bouton va incrémenter un compteur que l'on appellera c, et la valeur affichée v qui est calculée en appliquant une fonction de hachage de HMAC avec la clé privée k. Cette fonction est définie comme par K : V = HMAC (K, C).

Dans le cas de TOTP, on prend l'heure courante UNIX que l'on notera T, ramenée à des tranches de X secondes (souvent des tranches de 30 secondes) et on calcul par la formule : V = HMAC (K, T/X).

4.3.2.2 Le principe de l'authentification

Lorsque l'utilisateur décide de s'authentifier pour la première fois sur une application, il lui suffit de saisir sa clé privée et également de saisir la valeur affichée sur l'écran de son dispositif physique.

Le serveur est alors capable d'identifier la valeur initiale du compteur (HOTP) ou de l'horloge (TOTP). Par la suite, lorsque l'utilisateur aura besoin de s'authentifier à nouveau, il n'aura plus qu'à saisir la valeur affichée sur l'écran de son dispositif et le serveur sera capable de faire de lui-même le calcul afin de vérifier qu'il s'agit du bon code et s'il y a correspondance entre les deux codes.

C'est le même type de principe d'authentification que la YubiKey, un code généré à un moment T, n'est plus valable à un instant T+1. Dans le cas où la clé est subtilisée discrètement pour en extraire des valeurs et la remettre à sa place est inutile avec ce système.
La problématique suivante apparait alors avec ce type de système : comment le système peut-il faire correspondre le code fournit lors de l'authentification avec celui du dispositif si l'utilisateur s'est amusé à appuyer plusieurs fois sur le bouton ? Dans ce cas-là, les horloges du serveur et du dispositif (TOTP) ou du compteur (HOTP) ne sont plus synchronisé. Pour pallier à ce type de problématique, le serveur accepte une tolérance dans la valeur du compteur différente.

Pour cela, le serveur calcule X valeurs et la valeur saisie par l'utilisateur doit être parmi ces X valeurs.

Il vous faut donc disposer d'un dispositif HOTP par application. Sinon chaque authentification sur une application désynchroniserait le compteur côté serveurs des autres applications.

A l'inverse, avec un dispositif TOTP on peut l'utiliser sur autant d'application que l'on souhaite. Ceci à pour inconvénient que chaque application dispose de votre clé privée et pourraient donc s'authentifier à votre place sur d'autres applications.

4.3.2.3 Les avantages

Les dispositifs de type HOTP et TOTP ont été normalisés par des RFC[6], HOTP correspond à la norme 4226 et TOTP par 6238. Ces deux normes leurs permettent d'être implémenter et être disponibles sur un très grand nombre d'applications.

D'après nos recherches, il semblerait que ces deux types de technologies soient surtout utilisés par des professionnelles, comme par exemple des administrateurs systèmes.

Un autre avantage non négligeable est le prix de ce type de dispositif. Quelques dizaines d'euros, ce qui en fait, comme la solution YubiKey une solution abordable.

4.3.3 TOTP sur smartphone

4.3.3.1 Le principe de fonctionnement

À ce jour des solutions ont été mises au point pour générer du TOTP en version logicielle sur smartphone. Dans ce cas, la clé privée est intégrée dans le téléphone en faisant un scan d'un QR code.

L'inconvénient de cette nouvelle solution, est dans le cas où on perd, se fait dérober notre smartphone, on peut extraire la clé privée plus facilement que dans des solutions type YubiKey. Ainsi la personne qui nous a dérobé notre smartphone peut parvenir à s'authentifier sur nos applications.

On retrouve de plus en plus ce type de solution à ce jour. Google investit beaucoup sur ce type de solution, notamment par le biais du dispositif Google Authenticator.

L'application la plus connu actuellement pour générer du TOTP sur smartphone est sans contexte FreeOTP Authenticator disponible sur Android et iOS. Cette application vous permet de vous connecter sur des applications tels que : Amazon, GitHub, Facebook, etc …

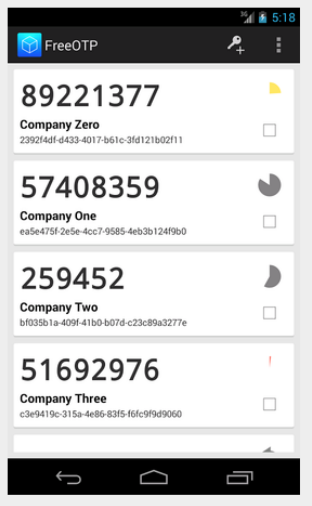

FIGURE 8 : REPRESENTATION DE L'APPLICATION FREEOTP AUTHENTICATOR

[6] Les RFC (Request For Comments) sont un ensemble de documents qui font référence auprès de la Communauté Internet et qui décrivent, spécifient, aident à l'implémentation, standardisent et débattent de la majorité des normes, standards, technologies et protocoles liés à Internet et aux réseaux en général.

4.3.3.2 Les avantages de cette solution

Il existe trois avantages indéniables sur la mise en place de ce type de solution :

1) La gratuité de l'application sur les différents terminaux existants à ce jour (Android / iOS).
2) Un nombre croissant de partenaires utilisant ce type de technologie.
3) Généralement on a plus facilement son smartphone sur soi que des YubiKey.
4) La facilité à mettre en place ce type de technologie : générer une clé privée via un QR code que l'on flash par la suite avec son téléphone.

4.3.4 Certificat X.509

4.3.4.1 Présentation de la norme X.509

La norme X.509 [14] est une norme de cryptographie basée sur ASN.1. Elle a été développée par l'union internationale des télécommunications en 1988 pour les infrastructures à clé publiques (PKI). C'est une norme complexe à mettre en place, employée essentiellement par HTTPS notamment par le biais de TLS.

Cette norme a établi un format standard de certificat électronique et un algorithme pour la validation de chemin de certification.

4.3.4.2 Fonctionnement de la norme X.509

Cette norme X.509 est utilisée par un navigateur pour authentifier un utilisateur de manière forte avec le serveur avec qu'il communique par l'intermédiaire de TLS/HTTPS.

Ceci permet de garantir à l'utilisateur l'authenticité du serveur avec lequel on communique.

Prenons le cas le plus extrême ou un utilisateur saisi des coordonnées bancaire sur un serveur qu'il n'est pas celui qu'il pense être. Cette norme permet donc d'éviter que ce type de tromperie existe. Cette garantie est fournie par de nombreuses certifications embarquées directement au sein du navigateur.

La norme X.509 permet une double authentification. Une première authentification du serveur sur lequel on réalise des opérations. Elle permet également au serveur de vérifier l'identité du client qui réalise une opération par le biais d'un « certificat client ».

Malheureusement, il semblerait que cette double vérification soit extrêmement complexe à mettre en place.

À ce jour, tous les projets tentant de mettre en place ce type de solution ont été un échec. Le dernier exemple en date est l'administration fiscale française en 2009.

4.3.4.3 Les avantages et inconvénients de cette norme X.509

Il existe trois véritables avantages à l'utilisation de cette norme :

1) Avec cette norme, nous pouvons créer sa propre autorité de certification, gérée par sa propre PKI, et tout certificat émis par cette autorité est valide et reconnu comme tel par le système.
2) Cette norme est implémentée nativement dans tous les navigateurs ainsi que dans les majorités des outils pouvant utiliser TLS (notamment les messageries instantanées, les logiciels de gestion de boite mail).
3) X.509 fournit tous les outils pour gérer la révocation d'un certificat (perte, départ, compromission, etc…).

Cette norme comporte quelques inconvénients dans son application et son exécution au quotidien :

1) Elle est extrêmement compliquée à mettre en place, seule quelques fonctionnalités sont véritablement gérées actuellement. Il semblerait que les développeurs ne parviennent pas à comprendre et à appliquer tout le potentiel de cette norme.
2) Elle est également difficilement comprise par les utilisateurs, elle demande une gestion régulière (renouvellement des certificats) et pose des problèmes techniques. Notamment l'importation de son certificat utilisateurs sur plusieurs machines, navigateurs, logiciels ne supportant pas ce mode de fonctionnement.

4.3.5 Les données biométriques

4.3.5.1 Présentation des données biométriques

Les données biométriques [15] sont des solutions d'identification et pas d'authentification comme par exemple les empreintes digitales, oculaires, palmaires etc.

Par définition, on doit pouvoir à tout moment révoquer une solution d'authentification. C'est-à-dire que vous pouvez facilement modifier votre mot de passe, reconfigurer votre dispositif physique (YubiKey, etc). Mais il est impossible de modifier des données biométriques.

Cependant, on s'aperçoit qu'aujourd'hui les données biométriques sont un complément lors de l'authentification. C'est notamment le cas des nouveaux smartphones. Les derniers smartphones inclus cette nouvelle disposition, malgré l'activation de cette authentification par données biométriques, certaines opérations demandent toujours la saisie d'un mot de passe (notamment lors de l'achat d'application, ou pour déverrouiller le téléphone lorsqu'il s'allume).

4.3.5.2 Un véritable complément d'authentification

Comme évoqué précédemment, les smartphones utilisent de plus en plus nos données biométriques pour nous identifier. On peut parier que ce type de données est de plus en plus utilisé car même s'il est possible de pirater nos données biométriques, cela reste tout de même très complexe à mettre en œuvre.

Cela est plus du domaine de la fiction d'arriver à pirater des données biométriques, tandis qu'il est possible de pirater un login d'utilisateur (notamment les techniques de « man in the middle », « phishing », etc).
De même il n'est pas suffisant d'utiliser simplement un dispositif physique sans un mot de passe et un compte utilisateur. Généralement il est même conseillé d'utiliser un mot de passe avec des critères particuliers (longueur, présences de caractères spéciaux, de chiffres, de majuscules etc …) pour parvenir à une authentification forte.

Conclusion

Durant la période de ce projet, nous avons enrichi nos connaissances relatives a :

- l'organisation de notre équipe et la répartition des tâches,
- au développement de compétences techniques

Les aspects les plus importants de ce projet ont été la collaboration, l'écoute, l'organisation du travail de groupe et le développement d'analyse et de techniques.

Ce projet a été pour nous une source de motivation alliant partie pratique (la mise en place d'une solution d'authentification et de cryptage) et partie théorique, analyse personnel et interprétation de notre expérience ainsi que de recherches et rédactions.

En effet durant ce projet nous avons pu véritablement faire le lien entre ces deux mondes (théorique et pratique) et ainsi mettre en concordance les notions apprises et acquises.

Toutes les études et analyses développées pendant notre cursus aussi bien Universitaire que Professionnel, avec notamment les cours de gestion de projet et base de données avancées que nous avons reçu en M1 ont été précieuses pour pouvoir gérer au mieux ce projet.

D'un point de vue technique, nous avons pris connaissance de l'importance de la cryptographie et surtout de la sécurité informatique pour y découvrir toutes les fonctionnalités, les finesses et leurs subtilités cela grâce à nos recherches et expériences personnelles.

Ces dernières sont être très utiles dans le domaine professionnel et cela nous a donné l'envie de le découvrir d'avantage et d'exploiter au mieux ses possibilités et fonctionnalités que nous n'avons pas maitrisées jusqu'ici et pour lesquels nous seront confrontées, demain, dans notre carrière professionnelle.

Nous avons été amenés à gérer un projet et ainsi avoir respecté des délais et faire des comptes rendus de l'état des lieux de nos travaux (développement, analyse, rédaction du rapport) auprès de nos partenaires et vous-même ce qui nous rendait responsable de notre travail.
Cela nous a permis également de mieux s'entraider, qui est une véritable valeur clé dans le domaine de l'entreprise mais également universitaire dans la mise en œuvre de tel projet.

En effet dès lors où nous rencontrons un dysfonctionnement, nous réfléchissions ensemble sur le problème afin de mettre en commun nos différentes idées et expériences pour y répondre. Ainsi les cours de gestion de projet et de communication nous ont permis de mieux encadrer notre travail afin d'aboutir au résultat escompté.

La communication était véritablement essentielle durant la réalisation de ce projet notamment par le biais de conférences, travaux en groupe à l'université ainsi que chez autrui car nous avons pu échanger, nous conseiller et nous guider et à anticiper les problèmes d'implémentation.

Ce pourquoi nous pensons aujourd'hui vous avoir rendu un travail le plus abouti possible même si nous avons rencontré quelques difficultés quant à la mise en place de nos idées. Le principal objectif nous le pensons a été de développer nos compétences en analyse en organisation et principalement une partie technique fournis par la découverte et redécouverte de l'aspect de sécurité informatique. Pour nous, tous ses objectifs ont été remplis avec succès.

Glossaire

L

La contre-mesure est l'ensemble des actions mises en œuvre en prévention de la menace. 3

La criticité est la détermination et hiérarchisation du degré d'importance et de la disponibilité du système d'information. 4

La menace représente une action capable de nuire à l'activité de l'entreprise. 3

La vulnérabilité est le niveau d'exposition face à la menace d'un système informatique. 3

Les RFC (Request For Comments) sont un ensemble de documents qui font référence auprès de la Communauté Internet et qui décrivent, spécifient, aident à l'implémentation, standardisent et débattent de la majorité des normes, standards, technologies et protocoles liés à Internet et aux réseaux en général. 17

O

On définit le risque par l'équation suivante : Risque = (Menace X Vulnérabilité) / (Contre-Mesure) 3

Table des illustrations

Webographie

[1]Marche-Public. Système informatique – data processing system. Disponible sur : http://www.marche-public.fr/Terminologie/Entrees/systeme-informatique.htm

[2]Wikipédia. Sécurité des systèmes d'information. Disponible sur : https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_des_syst%C3%A8mes_d'information

[3]Commentcamarche. Introduction à la sécurité informatique. Disponible sur : http://www.commentcamarche.net/contents/1033-introduction-a-la-securite-informatique

[4]CNIL. Vos obligations. Disponible sur : http://www.cnil.fr/vos-obligations/vos-obligations/

[5]Le bureau de conseil de la DCSSI (SGDN / DCSSI / SDO /BCS). La défense en profondeur appliquée aux systèmes d'information. Disponible sur : http://www.ssi.gouv.fr/uploads/IMG/pdf/mementodep-v1-1.pdf

[6]SSI. Disponible sur : http://www.ssi.gouv.fr/

[7]Searchsecurity. FIDO (Fast Identity Online). Disponible sur : http://searchsecurity.techtarget.com/definition/FIDO-Fast-Identity-Online

[8]Fido Alliance. Specifications Overview. Disponible sur : https://fidoalliance.org/specifications/overview/

[9]Zone-numerique. FIDO, une nouvelle méthode d'authentification proposée par des géants du high-tech. Disponible sur : http://www.zone-numerique.com/fido-une-nouvelle-methode-dauthentification-proposee-par-des-geants-du-high-tech.html

[10]Yubico. U2F-FIDO Universal 2ND Factor. Disponible sur : https://www.yubico.com/applications/fido/

[11] Wikipédia. Authentification forte. Disponible sur : https://fr.wikipedia.org/wiki/Authentification_forte

[12]Yubico. Yubikey4. Disponible sur : https://www.yubico.com/products/yubikey-hardware/yubikey4/

[13]Blog imirhil. De l'authentification sans mot de passe. Disponible sur : https://blog.imirhil.fr/2015/11/25/password-otp.html

[14]Wikipédia. X.509. Disponible sur : https://fr.wikipedia.org/wiki/X.509

[15]Securiteinfo. La Biométrie. Disponible sur : https://www.securiteinfo.com/conseils/biometrie.shtml