Herkens Antoine

Gillet Guillaume

Rapport Devoir N°2 SR03

Sommaire :

I-Introduction au projet

II-Bonnes pratiques de sécurité

III-Synthèse sujet de sécurité

IV-Conclusions et remarques personnelles

1. Intro
2. Bonnes pratiques de sécurité
3. Synthèse sujet de sécurité

L’authentification à deux facteurs, sécurité élevée, implémentation simple.

L’authentification à 2 facteurs est un moyen simple mais très efficace de sécuriser ses applis webs. Cela passe d’une application de banque à un compte sur un réseau social ou encore un compte sur une plateforme de jeu vidéo. Ce qui fait la puissance de cette authentification à 2 facteurs (ou A2F) est sa versatilité.

Comment cela fonctionne ? Le principe est simple, lorsque vous souhaitez vous connecter à votre compte sur le site/l’application web il vous est demandé d’entrer un code unique qui vient d’être généré, ce code, est reçu dans la plupart des cas sur votre smartphone par sms. Dans certains cas vous pouvez aussi le recevoir par mail. Dés lors tout est très simple, vous entrez le code reçu dans l’application et vous pouvez accéder à vos données en ayant très peu de chance de vous faire pirater votre compte car le pirate n’a pas accès à tous vos appareils comme votre réception de SMS.

Il existe un site qui recense tous les sites/applications qui utilisent cette méthode de sécurisation ( **[twofactorauth.org](https://twofactorauth.org/" \t "_blank)**. ).

Certains sites les plus aboutis en terme de sécurité ont amélioré cette méthode (notamment google et facebook), ils utilisent par exemple pour google votre smartphone ou tout autre appareil connecté à votre compte sur lequel une notification est envoyée demandant de valider la connexion du nouvel appareil en indiquant sa localisation est son nom/ip pour assurer de ne pas accepter de connexion malintentionnées.

Il existe aussi des applications dites « authenticator » qui permettent de générer en continu de nouveaux codes pour chaque compte de chaque application et le renouvellement de code en continu permet d’éviter les attaques par essais infinis (le code change tous les certains laps de temps). Et ces applications sont plus sures que des sms car elles sont gérées uniquement sur un terminal et les codes contrairement aux sms ne peuvent pas être interceptés par des pirates. Mais ils imposent une contrainte lors de la perte du terminal qui contient l’application, dans ce cas la personne le retrouvant pourrait si elle arrive a y accéder utiliser les codes de l’authenticator et entrer dans vos différents comptes.

Une nouvelle méthode d’authentification à deux facteurs à aussi vu le jour, elle utilise une clé usb externe qui une fois connectée à votre terminal va directement vous connecter de manière sécurisée à votre compte, mais pour cela il faut que l’application soit certifiée FIDO et accepte l’utilisation de cette clé U2F.

Finalement on remarque que l’authentification à 2 facteurs prend aujourd’hui différentes formes mais reste une norme qui se démocratise de plus en plus en sécurité, simple d’utilisation et d’implémentation elle réduit drastiquement les risques de piratage des données personnelles. Mais elle reste encore assez peu utilisée dans certains domaines et demande d’être activée manuellement lors du paramétrage des comptes utilisateurs, elle n’est pas obligatoire.

Vis-à-vis de l’application de banque on comprend qu’elle est très importante, elle est notamment utilisée lors des achats sur le net ou pour confirmer un virement. Par exemple lorsque vous utilisez votre carte bleue sur un site internet muni de cette technologie, il va vous être demandé un code, code envoyé par sms pour bien confirmer que c’est vous qui effectuez l’achat et que vous ne vous êtes pas fait voleé vos données de cartes bancaire.

Bien qu’efficace et facile à utiliser, cette authentification à deux facteurs se fait uniquement puissante lorsqu’elle est activée. Lors d’une fuite de données liée au piratage du serveur gérant l’application web, si les données personnelles de personnes n’ayant pas activé cette option fuitent, les pirates peuvent se donner à cœur joie de récupérer tout ce qu’ils peuvent au travers de l’application. Ce n’est donc pas une méthode de sécurité suffisante, elle doit être combinée avec d’autres méthodes notamment des encryptages côté serveur pour éviter le vol des données.

1. Conclusion