Description du travail

Le travail proposé concerne un système sécurisé de communication par l'intermédiaire d'un réseau basé sur des services cloud, donc je commence cette présentation par la description des problèmes majeurs existants dans le monde actuel et par la suite la solution proposée ;

Problématique

Tout le monde sait le problème de la sécurité informatique actuelle. L'arrivée de l'internet au monde ouvre un champ très vaste des services au gens tels que, possibilité de faire : des recherches, conversations, payement, travail et en plus le partage des données confidentielles en ligne.

Le problème parmi tous ces avantages et services offerts, on trouve des inconvenants qui menacent directement la sécurité des gens (internautes) (vie privée, données confidentielles, argent….) ; ce qu'on appelle par la sécurité informatique.

Jusqu'à maintenant, les gens font des progrès énormes, par l'utilisation des diffèrent techniques pour faire face contre ces menaces, on site par exemple ; des anti-virus, et des firewalls, des VPN, ….etc. Le problème c'est que le développement des mesures des sécurités engendre des développements des menaces informatiques et vis vers ça ; c'est à dire, le développement de nouvelles mesures de sécurité toujours se traduit par le développement des menaces plus puissant en parallèle. C'est pour ça, on trouve jusqu'à maintenant que les attaques informatiques trouvent toujours des chemins vers ses cibles ; parce que ;

- L'incapacité des anti-virus de faire face à tous les virus et les attaques informatiques ;
- Le problème des failles des systèmes, qui est un problème majeur des systèmes informatiques ;
- Le développement massive des virus sophistiqués que des fois même des Etats reste incapable de faire face contre eux ;
- La négligence des gens (internautes) lors de la navigation sur le Web ;

Le problème majeur que rencontrent tous les internautes et qui menaces leurs sécurité directement ; **c'est la navigation directe sur internet**, donc, la façon directe de faire piéger les internautes et propager les menaces informatiques (virus, …) c'est lors de la navigation des internautes sur le Web, vu que ce dernier (Web) présente un vrai menace, que même toutes les mesure de sécurité reste incapable de faire face contre ça.

La solution, réel qu'on peut le faire pour sécurise les internautes pour faire face contre les menaces sur le web, c'est de faire éviter la communication directe des internautes au web, et aussi éviter la réception des données reçue par le web directement sur les ordinateurs des internautes. Pour mieux expliquer ça ; imaginant un système intermédiaire qui reçoit les données et les scripts, en général, ce dernier (système intermédiaire) faire exécuter tout ça, et par la suite faire ***envoyer une capture d'écran à l'utilisateur***. Par cette méthode (système intermédiaire) on **sera sur** que l'internaute, va recevoir juste **un contenu propre** quel que soit le type des données communiquées par le serveur, puisqu'il reçoit par la suite juste une capture d'écran de ce dernier.

La technique présentée dans cette invention, et de faire connecter l'internaute au Web par l'intermédiaire d'un réseau qui offre une sécurité parfaite aux internautes par **l'isolement total du contact directe**. Je vais par la suite essayer d'expliquer le travail par des exemples ;

Une personne veut connecter sur le web, La solution actuelle c'est de faire passer les connexions à travers des anti-virus et des firewalls, ou bien des réseaux VPN. Ça veut dire les données de l'internet **sont reçus directement à l'ordinateur de l'internaute ; et l'exécution des scripts se font directement dans l'ordinateur des personnes, alors ; si l'antivirus n'est pas ajour, ou si le virus, n'est pas signalé dans les bases de données de l'antivirus, ou si le système d'exploitation présente des failles ou …. Alors, cette façon de communication présente un vrai danger pour la sécurité des internautes.**

Donc **le cœur du problème** c'est que les données arrivées du Web sont plantées directement dans les ordinateurs des internautes, et pour sécuriser l'internaute, il faut que ;

- L'anti-virus soit ajours et il détecte **tous** les virus (ca **pratiquement** c'est impossible) ;
- Le firewall soit assez fort pour bloquer toutes les connexions, (**pratiquement** impossible)
- Le système d'exploitation soit parfait, **aucune faille** (**pratiquement** c'est impossible) ;
- Tous les internautes ayant une culture de sécurité (**pratiquement** impossible) ;

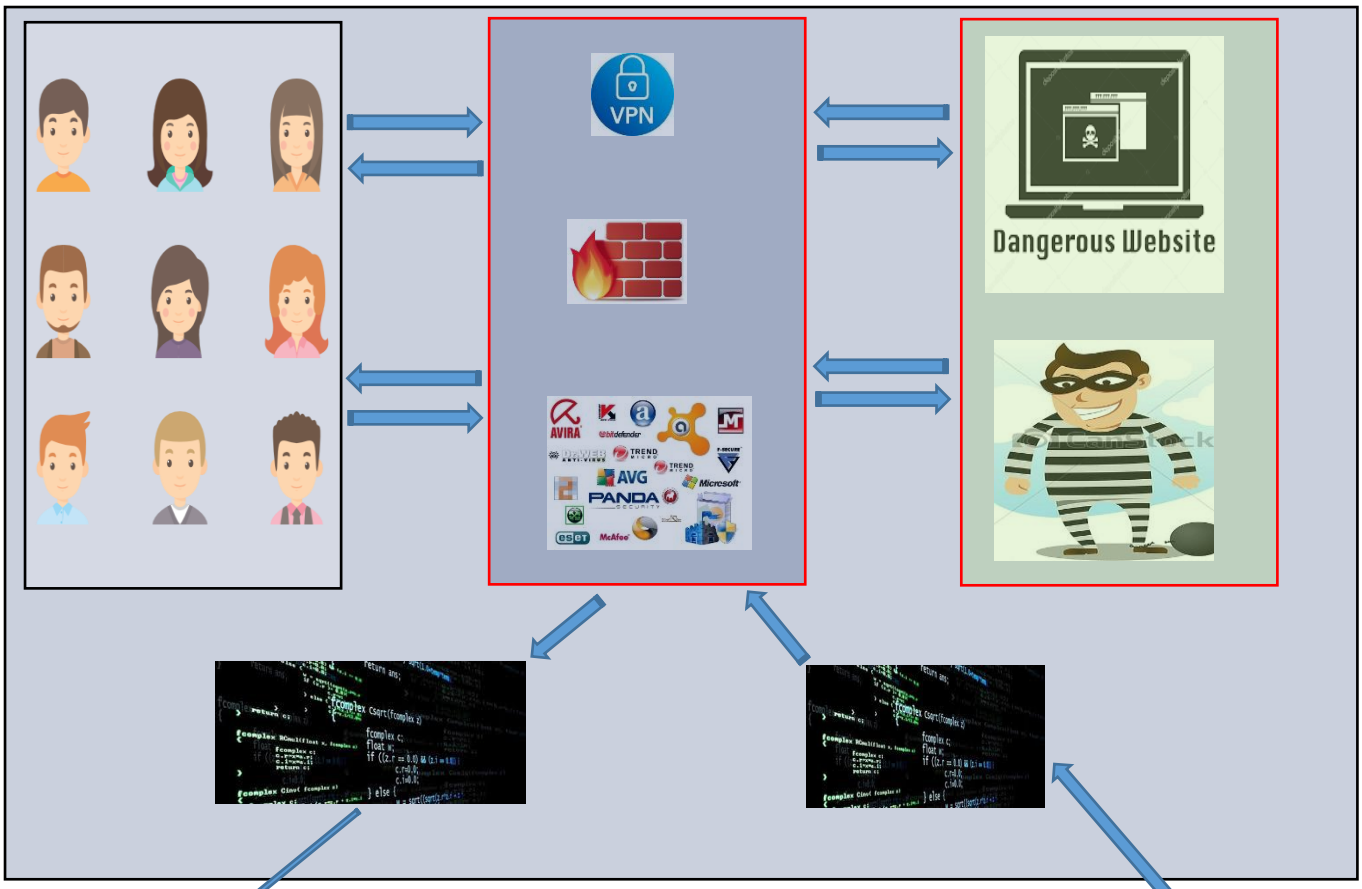
Le problème, c'est quelle que soit les mesures de sécurité prendre, c'est que les codes sources ou les scripts sont toujours exécutées dans les ordinateurs des internautes, alors, pour mettre l'internautes en toutes sécurité, il faut que toutes les **mesure des sécurité soient parfaites**, (lentivirus parfait, firewall parfait, système d'exploitation parfait) et ça, pratiquement c'est impossible.

Le schéma suivant, va décrire la solution actuelle, et la solution proposée.

Peoples

Mesures de sécurité

Web

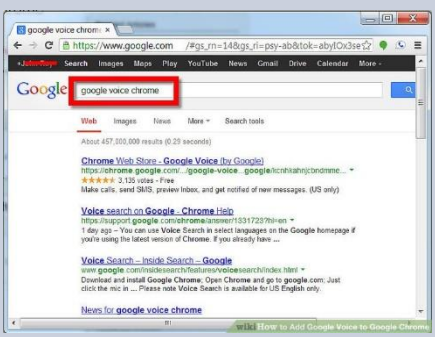


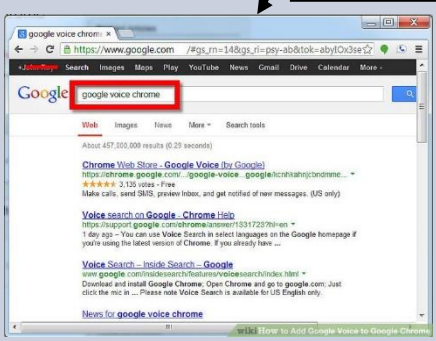
Solution actuelle

Contrôle (clavier +souris)

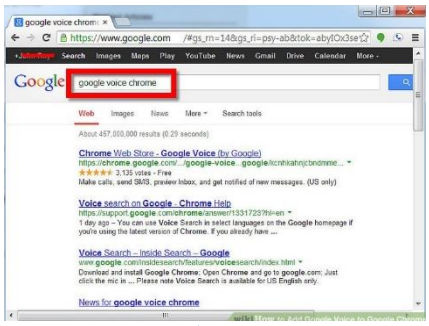
Capture d'écran

Script





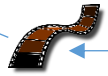
Solution proposée

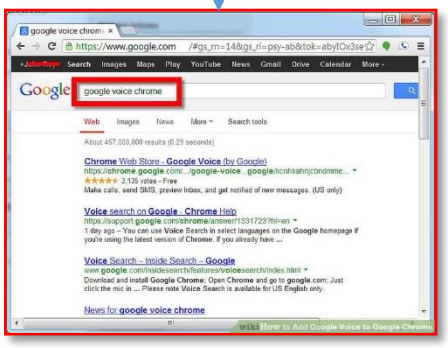


Script

Contrôle (clavier +souris)

Script





La solution proposée dans ce travail c'est de faire passer la connexion des internautes à travers un système intermédiaire et les données reçues sont pas reçues directement au computer de l'internaute, mais plutôt dans **le système intermédiaire,** et que cette dernière (internautes) reçoit juste une capture d'écran de ce qui se passe dans le réseau intermédiaire.

Donc le rôle du système intermédiaire c'est de faire recevoir les données envoyer par les différents serveurs Web et par la suite faire envoyer à l'internaute **juste une capture d'écran** de ce qui ce passe au niveau du système intermédiaire.

Par cette méthode on sera sur que les données reçues par le système intermédiaire seront propre et net, puisqu'il s'agit juste d'une capture d'écran de ce qui ce passe à l'intérieure du système intermédiaire ;

Donc, même si les différents serveurs Web envoie des virus ou des …. Ou essayent de faire des tentatives de piratage, **ça restant toujours juste dans le serveur intermédiaire**, même si le serveur intermédiaire reçoit un fichier virusé ou un lien virusé, et même si l'internaute clique sur ces fichiers ou ces liens, sont **ordinateur restent toujours intacte**, puisque tous les effets et les réactions reste au niveau du système intermédiaire.

La question maintenant c'est quoi ce système intermédiaire ?

La solution proposée par cette invention, s'agit, **d'un service au cloud**, donc pour faire marcher ce Système, on est besoin de deux service ;

- **Un service au niveau d'internaute ;**
- **Un service au niveau du cloud ;**

- ***Un service au niveau d'internaute***

Il s'agit d'un logiciel de commande, qui a la même fonction ; par exemple d'un ***TeamViewer***,

- ***Un service au niveau du cloud ;***

On installe le service ou programme qu'on veut l'exécuter sur cloud, par exemple un browser comme ou Mozilla Firefox ; Google chrome…etc.

Alors, lorsqu'on clique sur le logiciel de commande installé au niveau de l'ordinateur d'internaute, il va faire exécuter le programme installé sur le cloud et de le faire ouvrir directement sur le service cloud, **du coup, l'internaute va voire une fenêtre directe du browser installé sur le service cloud.**

Donc, l'internaute **sent qu'il travaille sur un browser qui est installé sur son pc, mais réellement le browser il est le cloud.** Mais l'internaute il a juste la commande a travers du logiciel de commande.

Alors, n’importe quel chose passe sur le cloud (réception des virus, tentative de piratage, des liens mal veillent …) son effet reste toujours sur le système intermédiaire (ca veut dire le cloud)

L’internaute il a aussi la possibilité de redémarrer le cloud à chaque fois et vider la cache (RAM) du cloud, a lors la réinitialisation de toutes les donnée, (ca veut dire même si le système cloud il sera infecter, une simple réinitialisation du cloud va vider tous (c’est même fonction comme le logiciel Deep-freez).

En plus en peut ajouter des mesure de sécurité au cloud, comme ; firewall, un système VPN, un antivirus) pour améliorer la sécurité du cloud, mais pour ce travail, ce n’est pas ça le but. (Puisque la solution est déjà existante).

Le but c’est de faire communiquer avec ‘le Web par un système intermédiaire, le but du système intermédiaire c’est de faire exécuter toute les scriptes et interagir avec les différents serveurs du monde, et de faire envoyer au internaute un contenue parfaitement propre (vu qu’il envoie à internaute juste un capture d’écran et un enregistrement vidéo).